ГОСТ 7.32-2001

НАУЧНО-ОБРАЗОВАТЕЛЬНЫЙ ЦЕНТР КОМПЕТЕНЦИЙ В ОБЛАСТИ ЦИФРОВОЙ ЭКОНОМИКИ МГУ ИМЕНИ М.В. ЛОМОНОСОВА

УДК 004 (470+571)

УТВЕРЖДАЮ
директор Научно-
образовательного центра компетенций
в области цифровой экономики МГУ
имени М.В. Ломоносова
_____ к. э. н. Т.В. Ершова
«___» _____ _____ г.

ОТЧЕТ
О НАУЧНО-ИССЛЕДОВАТЕЛЬСКОЙ РАБОТЕ
по теме:

Проблемы управления правами на результаты интеллектуальной деятельности, непосредственно связанные с личностью физического лица

Руководитель темы _____ Дмитрик Н.А.

Москва
2018

СПИСОК ИСПОЛНИТЕЛЕЙ

Руководитель темы _____ Н.А. Дмитрик, консультант Центра хранения и анализа больших данных Научно-образовательного центра компетенций в области цифровой экономики МГУ имени М.В. Ломоносова

Ответственный исполнитель _____ д.т.н. А.Н. Райков, научный сотрудник Научно-образовательного центра компетенций в области цифровой экономики МГУ имени М.В. Ломоносова

Исполнитель _____ С.В. Зива, научный сотрудник Научно-образовательного центра компетенций в области цифровой экономики МГУ имени М.В. Ломоносова

Проблемы управления правами на результаты интеллектуальной деятельности, непосредственно связанные с личностью физического лица НИР

Managing Intellectual Property Rights Directly Related to the Personality of an Individual

Руководитель НИР: Дмитрик Н.А.

Ответственный исполнитель: Райков А.Н.

Подразделение: Научно-образовательный центр компетенций в области цифровой экономики

Срок исполнения: 1 января 2018 г. - 31 декабря 2018 г.

Ключевые слова: результаты интеллектуальной деятельности, персональные данные, управление интеллектуальными правами, право гражданина на изображение

citizen's right to an image, intellectual property rights, managing intellectual property rights, personal data

РЕФЕРАТ

Объектом исследования являются общественные отношения, возникающие при создании и использовании результатов интеллектуальной деятельности, непосредственно связанных с личностью физического лица, а также при распоряжении правами на такие результаты интеллектуальной деятельности.

Целью исследования является совершенствование инструментов и механизмов контроля физического лица за обработкой относящейся к нему информации.

В результате работы был проведен комплексный анализ системы правового регулирования отношений по обеспечению неприкосновенности частной жизни, по обработке персональных данных и распоряжению правами на персональные данные. В предмет анализа вошло регулирование указанных отношений в РФ и странах бывшего СССР. По результатам работы были предложены изменения в законодательство в целях создания условий для управления правами на результаты интеллектуальной деятельности, непосредственно связанные с личностью физического лица.

ВВЕДЕНИЕ

Настоящее исследование посвящено совершенствованию инструментов и механизмов контроля физического лица за обработкой относящейся к нему информации. Сейчас для реализации такого контроля используются как гражданско-правовые (интеллектуальная собственность, право на изображение), так и административно-правовые (персональные данные) механизмы. Одной из главных проблем, возникающих в существующей системе контроля, является плохая совместимость гражданско-правовых и административно-правовых инструментов. Административные механизмы направлены на приоритетное обеспечение интересов государства и, как следствие, не рассчитаны на рыночное использование РИД, связанных с личностью физического лица. Гражданско-правовые механизмы пока не обеспечивают агрегирование прав в объеме, достаточном, чтобы эффективно управлять ими на рынке, монополизированном транснациональными корпорациями и компаниями госсектора.

В настоящем исследовании в целях разработки системы инструментов и механизмов контроля физического лица за обработкой относящейся к нему информации был проведен анализ следующих проблемных вопросов:

- анализ прав на персональные данные как разновидности интеллектуальных прав;
- определение места прав на результаты интеллектуальной деятельности, непосредственно связанные с личностью физического лица, в системе правового регулирования, в том числе в системе прав на информацию;
- описание правового регулирования данных, связанных с личностью физического лица, в странах бывшего СССР.

По результатам проведенного анализа были предложены изменения в действующее законодательство.

ОСНОВНАЯ ЧАСТЬ

1. ПРАВО НА ПЕРСОНАЛЬНЫЕ ДАННЫЕ КАК РАЗНОВИДНОСТЬ ИНТЕЛЛЕКТУАЛЬНЫХ ПРАВ

Статья 9 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (далее – Закон о персональных данных) описывает, что представляет собой согласие на обработку персональных данных. Законодатель указывает, что согласие на обработку отражает решение субъекта персональных данных о предоставлении его персональных данных. Согласие дается субъектом свободно, по своей воле и в своем интересе; конкретно, информированно и сознательно. Согласие на обработку персональных данных может быть дано субъектом персональных данных или его представителем в любой позволяющей подтвердить факт его получения форме, если иное не установлено федеральным законом. Конституционной основой конструкции «данные – гражданин – согласие» выступает статья 23 Конституции Российской Федерации, устанавливающая, что сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются.

Упоминания о согласии гражданина на обработку данных о нем, однако, не было в Конституции СССР 1977 года (Статья 56 «Личная жизнь граждан, тайна переписки, телефонных переговоров и телеграфных сообщений охраняются законом»). Не говорится про согласие на обработку данных о гражданине и в основополагающих международных документах:

- статье 12 Всеобщей декларации прав человека 1948 года («Никто не может подвергаться произвольному вмешательству в его личную и семейную жизнь, произвольным посягательствам на неприкосновенность его жилища, тайну его корреспонденции или на его честь и репутацию. Каждый человек имеет право на защиту закона от такого вмешательства или таких посягательств»);

- статье 8 Европейской конвенции по правам человека («Каждый имеет право на уважение его личной и семейной жизни, его жилища и его корреспонденции»);

- Конвенции Совета Европы ETS N 108 о защите физических лиц при автоматизированной обработке персональных данных.

Как видно из текста перечисленных актов, они устанавливают принципы и подходы к обработке данных о гражданине независимо от наличия или отсутствия согласия гражданина. Появилось же согласие гражданина на обработку данных о нем в его современном виде только в Руководящих принципах Организации экономического сотрудничества и развития 1980 года, регулирующих неразглашение и трансграничные

потоки личных данных (далее – Руководящие принципы ОЭСР), а через шестнадцать лет – в Директиве Европейского Парламента и Совета Европейского Союза 95/46/ЕС от 24 октября 1995 г. о защите физических лиц при обработке персональных данных и о свободном обращении таких данных (далее – Директива 95/46/ЕС).

Причины того, что в течение долгого времени согласие гражданина (или его отсутствие) не принималось в расчет при установлении принципов неприкосновенности частной жизни, лежат в истоках возникновения самого права на неприкосновенность частной жизни, которое, в свою очередь, появилось вслед за правом на приватность (privacy). Основополагающей работой для того, что в американской правовой традиции называется privacy, является статья Samuel D. Warren и Louis D. Brandeis «The right to privacy», где право на приватность было впервые обосновано и с позиций общего права (common law), и de lege ferendae. Общее право еще с конца XVIII века признавало наличие у гражданина права контролировать «выражение мыслей», то есть самому решать, делать личностные проявления (такие как дневники, письма, заметки) публичными или нет . Однако суды расходились в обосновании для этого права: разновидность ли это права собственности, контракта или траста? Воррен и Брандейс выступили с утверждением, что право на приватность не может черпать свою силу ни из права собственности (потому что в нарушении приватности может и не быть экономического интереса), ни из контракта или траста (потому что право на приватность – это «право против всего мира», а не только против стороны по договору или трасту, действительному или предполагаемому).

Однако создатели права на приватность строили его по образу и подобию права интеллектуальной собственности. Более того, одним из аргументов в пользу права на приватность было то, что выражение мыслей в обычной жизни, часто в непроизвольной манере (в поведении, разговоре, образе жизни и т.п.) должно защищаться правом в том же объеме, что и намеренное выражение мыслей в произведениях науки и искусства. «Если брать за основу трудозатраты, то можно найти, что усилия по правильному поведению в домашних и бизнес-отношениях гораздо выше, чем те, которые необходимы, чтобы нарисовать картинку или написать книгу; легче выражать мысли в дневнике, чем вести достойную жизнь. Если брать за основу намеренность поведения, то большинство обычной корреспонденции, которая в настоящее время пользуется <правовой> охраной, будет исключена из сферы применения существующих правил»[1]. Поэтому на этапе возникновения права на приватность согласие на обработку информации о гражданине – аналогично лицензии на использование произведения – было неотъемлемым элементом данного права, хотя само право и было направлено в сторону, противоположную любой собственности, в том числе интеллектуальной. В дальнейшем, правда, нематериальное право на приватность и права, охраняющие экономический интерес в информации о гражданине, в общем праве разделились, чему способствовало появление в американском законодательстве «прав знаменитостей» (celebrity rights). Эти права, имеющие экономическое содержание и являющиеся полноценной разновидностью интеллектуальной собственности, позволяют выдавать лицензии на использование образа знаменитостей и даже могут переходить по наследству[2].

В Европе право на приватность развивалось иначе. Как отмечает Хью Беверли-Смит, составителям Германского Гражданского Уложения (ГГУ) была известна общая концепция «персональных прав» (то есть прав на определенную информацию о себе – имя, изображение, информация о частной жизни), но они ее отвергли, как чересчур туманную[2]. В результате к вопросу об общем «персональном» праве гражданина в Германии смогли вернуться только в 1950-е, уже после принятия Основного закона ФРГ и Европейской конвенции по правам человека. Во Франции статья 9 французского гражданского кодекса, посвященная охране частной жизни, была введена только в 1970 году – и также не предусматривает института согласия гражданина на обработку данных о нем. Институт неприкосновенности частной жизни в Европе, таким образом,

формировался уже после Второй мировой войны, а за основу бралось отнюдь не авторское право, как в сытой буржуазной Америке конца XIX века. Право на неприкосновенность частной жизни в Европе – это неотъемлемое право личности, выстраданное в тоталитарном нацистском государстве и отвоеванное в двух мировых войнах[3]. Поэтому это право на уважение к частной жизни, на формирование неприкосновенного пространства, «внутреннего круга», – а не право торговать данными о своей частной жизни.

В аналогичном ключе понималось право на неприкосновенность личной жизни и в Советском Союзе. Гарантированное статьей 56 Конституции СССР право на охрану личной жизни граждан относилось к личным неимущественным правам[4]. При этом, как отмечает М.Н. Малеина, хотя личные неимущественные права охраняются несколькими отраслями права, «субъективное личное неимущественное право не зависит от того, нормами скольких и каких именно отраслей права осуществляется его защита, и не теряет своей отраслевой принадлежности. … Нематериальный характер личных прав проявляется в том, что они лишены экономического содержания. … Объектами неимущественных прав могут выступать нематериальные (духовные) блага, неотделимые от личности – имя, честь, достоинство, здоровье, тайна личной жизни и др.»[4]. В советской правовой науке даже была точка зрения (правда, не всеми разделяемая), что отношения по поводу нематериальных благ, не связанных с имущественными, правом не регулируются, а только охраняются[5]. «Закон не определяет активных действий, которые мог бы совершить управомоченный, а указывает лишь на неприкосновенность соответствующих личных благ и на способы защиты»[4].

Однако в советской правовой науке неотчуждаемость нематериального блага отнюдь не связывалась с невозможностью отчуждения (полного или частичного) соответствующего личного неимущественного права. М.Н. Малеина, в частности, говоря о возможности перехода (отчуждения) субъективных неимущественных прав и отдельных правомочий, составляющих их содержание, ссылалась на известную цитату Г.Ф. Шершеневича, что «субъективное право есть средство для обеспечения пользования благами, но последние также мало принадлежат к понятию прав, как сад к садовой ограде»[4].

Упоминание согласия гражданина на обработку данных о нем в Руководящих принципах ОЭСР; согласие субъекта как условие prima facie обработки персональных данных в Директиве 95/46/ЕС; наконец, упоминание согласия гражданина на сбор, хранение, использование и распространение информации о его частной жизни в российской Конституции, - все это признаки понимания учеными и политиками того факта, что данные о гражданине отчуждаются от него. Более того, забегая вперед, скажем, что такое отчуждение является неотъемлемым условием нормального гражданского оборота и нормальной общественной жизни в государстве. Однако к моменту, когда согласие было возвращено в список условий обработки персональных данных, сам этот институт в западной правовой традиции достаточно прочно обосновался в сфере публичного, а не частного права. В России ситуация еще более странная: гражданское законодательство (особенно со вступлением в силу статьи 152.2 Гражданского кодекса РФ) выполняет охранительную функцию в отношении частной жизни гражданина, но при этом оборот персональных данных, регулируемый Законом о персональных данных, к сфере действия гражданского законодательства не относится. Казалось бы, должно быть наоборот: оборот должен регулироваться гражданским правом, а охрана осуществляться уголовным, административным и иным публичным.

Принципиальным для понимания правовой природы согласия на обработку персональных данных вопросом является вопрос о позиционировании данного института в системе публичного или частного права (в объективном смысле этого слова) и в системе имущественных или неимущественных прав (в субъективном смысле). К сожалению,

Закон о персональных данных не дает на этот вопрос прямого ответа, устанавливая только (статья 2), что его целью является обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну. Оговорка «в том числе» позволяет говорить о данном акте как о комплексном, содержащем в себе нормы разных отраслей законодательства.

Рассматривая вопрос о том, лежит ли институт согласия на обработку персональных данных в поле публичного права, нельзя не отметить, что как частному, так и публичному праву известно согласие как правовое средство. Так, пункт «а» статьи 83 Конституции РФ предусматривает, что Президент Российской Федерации назначает с согласия Государственной Думы Председателя Правительства Российской Федерации. Пункт 41.1 статьи 5 Уголовно-процессуального кодекса РФ устанавливает, что согласие – это разрешение руководителя следственного органа на производство следователем или разрешение прокурора, начальника органа дознания на производство дознавателем соответствующих следственных и иных процессуальных действий и на принятие ими процессуальных решений. Таким образом, в публичном праве согласие, как правило, выступает одним из проявлений отношений власти и подчинения, наличия полномочий по регулированию в той или иной сфере.

В трудовом праве как отрасли частного права согласие работника требуется в различных случаях изменения трудового договора (например, совмещения должностей, перевода на другую работу и т.п.). Необходимость получения согласия в данном случае обусловлена тем, что, в соответствии со статьей 56 ТК РФ, трудовой договор - это соглашение между работодателем и работником. Изменение трудового договора возможно по согласию его сторон.

В гражданском праве случаи получения согласия обширны и многочисленны. Гражданский кодекс РФ (далее – ГК РФ) говорит и о согласии на использование имени гражданина (статья 19), и о согласии законных представителей на совершение сделок несовершеннолетним (статья 26), и о согласии уполномоченных государственных органов на осуществление реорганизации юридического лица (статья 57), и о согласии участников общества или его органов на совершение сделок (статья 72), и о многих других. Однако во всех случаях согласие является проявлением каких-либо прав: родительских, корпоративных, права собственности или опять-таки властных полномочий (в случае, когда требуется согласие уполномоченного органа на реорганизацию).

Если задаться вопросом, на каком праве основано согласие на обработку персональных данных, мы вернемся к тому, с чего более ста лет назад начинали Воррен и Брандейс: право на приватность основано на праве собственности, договоре или чем-то еще? И если ответить, что в основе согласия – личное неимущественное право на нематериальное благо (информацию о частной жизни лица), то почему согласие дается на использование такой информации? Если руководствоваться принципом «нельзя передать больше прав, чем имеешь сам», получается, что и само по себе право на неприкосновенность частной жизни – это право на использование такой информации? Ведь именно этим – передачей возможности использования блага – отличается согласие на обработку персональных данных от, например, согласия на совершение сделок или на эмансипацию.

Из проведенного выше анализа следует вывод о выборе места института согласия на обработку персональных данных не только между публичным и частным правом, но и между имущественными и личными неимущественными субъективными правами. Если правомочие давать согласие на обработку данных о себе не основано на отношениях власти и подчинения, ему не место в системе публичного права. Тем более этот институт должен быть в сфере частного права, если он является отражением не нематериального

(или не только нематериального), но и материального, имеющего экономическую ценность блага. Здесь стоит еще раз напомнить, что в силу пункта 1 статьи 2 ГК РФ, предметом регулирования гражданского законодательства являются имущественные и личные неимущественные отношения, основанные на равенстве, автономии воли и имущественной самостоятельности участников. Наличие же в праве гражданина на данные о своей частной жизни как личного неимущественного, так и имущественного компонента, не мешает осуществлять регулирование процесса его осуществления в рамках гражданского права. Как справедливо указывает на этот счет М.Н. Малеина: «Личные неимущественные права, связанные с имущественными, при их реализации могут выступать в качестве предпосылки возникновения имущественных прав»[4].

Нельзя не отметить сходство между субъективным правом, на котором основано правомочие давать согласие на обработку персональных данных, и исключительным правом. «Исключительность такого рода субъективных гражданских прав состоит в том, что право на данный конкретный объект может принадлежать лишь определенному лицу или организации, указанному в законе или ином государственном акте, например, в патенте на изобретение, в акте регистрации товарного знака и др.»[6]. Причем, как справедливо отмечает А.Ю. Кувыркова, исключительное право является правом с положительным содержанием. «Разумеется, по своей сути исключительное право – это «право исключать», «право воспрещения», право устранять всех иных лиц от использования объекта. Но это не означает, что исключительное право сводится только к возможности запрещать: ведь целью установления исключительных прав было введение данных прав в гражданский оборот, то есть возможность получать вознаграждение за предоставление прав на использование объектов иным лицам. Если мы понимаем под исключительным правом лишь право запрещать, то получается, что вознаграждение будет уплачиваться за отказ от осуществления права, что противоречит сути и смыслу гражданско-правовой охраны. Поэтому исключительное право – это право и разрешать (что необходимо для введения права в гражданский оборот), и запрещать (что необходимо для защиты интересов правообладателя)»[7].

Конечно, до включения персональных данных в статью 1225 ГК РФ, нельзя говорить о том, что персональные данные являются интеллектуальной собственностью. Принципиальное отличие между персональными данными и интеллектуальной собственностью в настоящее время проявляется, например, в невозможности отчуждения «исключительного» права на персональные данные или выдачи исключительной лицензии на их использование. Однако понимание того, что данный институт был не просто так построен по образу и подобию института авторского права, способно помочь в регулировании и использовании данного института. Понимание согласия на обработку персональных данных как сделки или даже договора позволяет поставить вопрос о его действительности или недействительности (в настоящий момент согласие нельзя признать недействительным), в том числе по основаниям, связанным с формой такого согласия. Применение положений статьи 421 ГК РФ о свободе договора позволяет сторонам самостоятельно структурировать отношения по обработке персональных данных, прежде всего, в части вознаграждения за предоставленное согласие на обработку персональных данных. Понимание права на свои персональные данные как полноценного субъективного гражданского права дает возможность в полной мере использовать как средства защиты, предусмотренные статьей 12 ГК РФ, так и пределы осуществления гражданских прав, установленные в статье 10 ГК РФ. При этом для осуществления и защиты прав могут быть использованы все те фактически сложившиеся формы, которые существуют в области интеллектуальной собственности: например, организации по коллективному управлению правами. Фактически, только такие организации смогут стать игроками на рынке, достаточно мощными, чтобы противостоять крупнейшим мировым агрегаторам персональных данных, прежде всего соцсетям .

Здесь, однако, необходимо сделать важную оговорку о том, что является объектом такого права. Сведения о гражданине, персональные данные намного шире, чем неприкосновенность частной жизни, личная и семейная тайна, иные аналогичные нематериальные блага, принадлежащие гражданину от рождения или в силу закона, которые неотчуждаемы и непередаваемы иным способом в силу статьи 150 ГК РФ. Однако перечисленные в указанной статье блага не просто так выделены в круг неотчуждаемых и непередаваемых; как не просто так выведены из сферы действия Закона о персональных данных отношения по обработке персональных данных физическими лицами исключительно для личных и семейных нужд, если при этом не нарушаются права субъектов персональных данных. Частная жизнь потому и является частной, что она находится вне пределов правового регулирования: здесь действуют нормы морали, обычая, но не права. Поэтому неизбежное сближение законодательства о персональных данных с законодательством об интеллектуальной собственности не повлечет никаких изменений для неприкосновенности частной жизни: право будет только предоставлять охрану данной сфере от возможных посягательств, но не регулировать вторжение в нее.

Также нельзя не отметить, что правовой режим отдельных видов того, что сейчас подпадает под понятие персональных данных, может сильно разниться. Так, самостоятельные нормы установлены для имени гражданина (статья 19 ГК РФ), его электронной подписи (Федеральный закон от 06.04.2011 №63-ФЗ «Об электронной подписи»), идентификационного номера налогоплательщика (статья 84 Налогового кодекса РФ), СНИЛС (статья 6 Федерального закона от 1 апреля 1996 г. № 27-ФЗ «Об индивидуальном (персонифицированном) учете в системе обязательного пенсионного страхования») и других. Все перечисленные виды информации являются идентификаторами, позволяющими определить гражданина как субъекта права и субъекта конкретных правоотношений. Нельзя говорить о том, что вопрос об использовании идентификатора относится на усмотрение самого гражданина, а следовательно, использование идентификаторов не является предметом согласия на обработку персональных данных в тех случаях, когда идентификатор нужен собственно для идентификации (стороны по договору, управомоченного или обязанного лица и т.п.). Поскольку для каждого идентификатора законом установлен свой режим, он-то и должен применяться. Распространение на использование идентификаторов правового режима персональных данных только приводит к коллизиям (самая известная: необходимость получения согласия генерального директора организации на обработку его ФИО при заключении договора с организацией), не создавая никаких благ для идентифицируемых лиц.

Как уже отмечалось выше, в субъективном праве на персональные данные неразрывно соединены имущественный и неимущественный компоненты. Но предоставление согласия на обработку персональных данных является одновременно способом осуществления как имущественного, так и неимущественного права, а посему не требуется отдельного регулирования имущественного и неимущественного компонента. Тем не менее, вопрос о том, какая сторона – имущественная или неимущественная – приоритетна, имеет определенное значение с точки зрения объекта данного права. Если исходить из приоритета нематериального блага, в состав объектов права должно включаться максимальное число сведений. Если же брать за основу регулирования материальную составляющую, то перечень сведений, входящих в объем права неоправданно сузится, поскольку лишь немногие из них могут быть объектом товарных отношений. Для того, чтобы найти баланс, можно предложить следующий подход. Объектом исключительного права считаются данные о физическом лице, интерес в обработке которых обусловливается тем, что они относятся к этому лицу. Если данные обрабатываются вне связи с неким субъектом, пусть даже определяемым с использованием этих данных, согласие на их обработку не требуется. Например, если на

компьютерной панораме улицы оказываются запечатлены прохожие, их согласие на публикацию панорамы не потребуется, так как у создателя панорамы нет интереса в обработке данных о конкретных физических лицах, ему нужна именно панорама улицы.

Подводя итог сказанному выше, можно заключить, что согласие на обработку персональных данных является способом осуществления исключительного права физического лица на данные, интерес в обработке которых обусловливается тем, что они относятся к этому лицу. Хотя в настоящий момент отношения по осуществлению данного права подвергаются комплексному регулированию, включающему в себя элементы частного и публичного права, необходимо выводить такие отношения из сферы публичного права и осуществлять унификацию норм о персональных данных с нормами законодательства об интеллектуальной собственности. При этом должен сохраняться объем правовой охраны неприкосновенности частной жизни как сферы, находящейся за пределами правового регулирования, а для идентификаторов должен сохраняться тот правовой режим, который устанавливается специальными нормами, относящимися к таким идентификаторам.

СПИСОК ИСТОЧНИКОВ:

1. Warren S.D., Brandeis L.D. The Right to Privacy. // Harvard Law Review, 1890, №4.

2. Beverley-Smith Huw. The commercial appropriation of personality. Cambridge University Press, 2002.

3. Steiner H.J., Alston P. International human rights in context. Oxford, 2000.

4. Малеина М.Н. Личные неимущественные права. М., 1990.

5. Гражданско-правовая охрана интересов личности /Отв. ред. Черепахин Б.Б. М., 1969.

6. Грибанов В.П. Осуществление и защита гражданских прав. М., 2001.

7. Кувыркова А.Ю. Осуществление исключительных интеллектуальных смежных прав. Дисс. … канд. юр. наук. М., 2010.

2. МЕСТО ПРАВ НА РЕЗУЛЬТАТЫ ИНТЕЛЛЕКТУАЛЬНОЙ ДЕЯТЕЛЬНОСТИ, НЕПОСРЕДСТВЕННО СВЯЗАННЫЕ С ЛИЧНОСТЬЮ ФИЗИЧЕСКОГО ЛИЦА, В СИСТЕМЕ ПРАВОВОГО РЕГУЛИРОВАНИЯ

Отечественная правовая наука по преимуществу стоит на позитивистских устоях. Если в работах по теории права непозитивистские теории еще рассматриваются (но позитивистская, или нормативная – обязательно на первом месте) [1, с.168-172; 2, с.12], то прикладные исследования, посвященные специальным вопросам, как правило, представляют собой лишь анализ норм правовых актов и судебной практики. Причин у сложившейся ситуации много: отчасти это советское наследие, отчасти – особенность правосознания современных чиновников и политических деятелей.

Отправной точкой для работ советского периода служили тезисы В.И. Ленина о том, что «закон есть выражение воли классов, которые одержали победу и держат в своих руках государственную власть», а «право есть ничто без аппарата, способного принуждать к исполнению норм права» [3, с.76]. Нормативность признавалась сутью права, его определяющим объективным свойством [4, с.21; 5, с.43-45]. Работы исследователей, указывавших, что «право существует постольку, поскольку оно соприкасается с сознанием субъекта, реципиента правового веления», нещадно критиковались [6]. «Закон, после того, как он издан и вступил в силу, обладает относительной самостоятельностью –

он действует независимо от воли и сознания того, кому он адресован, независимо от реципиента. Но это возможно лишь потому, что имеется аппарат принуждения к выполнению норм права, имеется механизм» [5, с.45].

На корни современного позитивизма указывал С.С. Алексеев. «В нашей стране, начиная с 1990-х гг. и все более и более в последующее время даже сам термин «право» стал исчезать из официальной лексики. Центр тяжести стал все более переноситься на категорию «закон» (трактуемый во многом по модели «инструкции», произвольно определяемой властью)» [7, с.16-17]. Обращают внимание на эту закономерность и исследователи, не являющиеся юристами: «Тогда как Запад … основывается на духе закона, Россия формально следует букве закона». «Кажется, очень важно было … следовать формальному закону и обосновывать свои действия соответствием писаным нормам, обращая меньшее внимание на другие аспекты правового и политического процесса» [8, с.759, 761].

Юристы с самого первого курса в университете учатся воспринимать право как данность, как императив. Дальнейшая работа только укрепляет нас в этом ощущении: составляя договор или справку по законодательству, мы опираемся на нормы закона, подзаконных актов, судебные решения, пытаясь определить предписанный нам государством вариант поведения. Но чем больше позитивизм проникает в наше профессиональное сознание, тем острее становятся видны проблемы, вызванные нормативным подходом к праву. Это и проблема злоупотребления правом («как может осуществление права быть противоправным?»), и проблема «каучуковых норм» (принцип разумности, добросовестности и т.п.), и проблема правовых гарантий (как может одна правовая норма считаться гарантией другой, столь же правовой, нормы?). В самом общем виде столкновение такого рода «неразрешимых» правовых проблем с позитивистским мышлением выразил В.И. Емельянов в своей работе о злоупотреблении правом: «С точки зрения сторонников введения в закон понятия пределов осуществления права, существует два уровня дозволений». И далее: «Совокупность правовых норм, ограничивающих субъективное право, не создает другой идеальной модели поведения, отличной от той, которая установлена управомочивающей нормой. Мера дозволенного поведения (субъективное право) остается единой. Нельзя говорить, что этими нормами устанавливаются «пределы осуществления субъективного права». В то же время, именно на наличии двух мер поведения основано приведенное выше определение понятия «злоупотребления гражданскими правами» [9, с.54-55]. И действительно, если все право позитивно, все правила поведения связаны между собой, все субъективные права раз и навсегда определены законодателем, – наличие норм «второго порядка», таких как запрет злоупотребления правом, запрет недобросовестного поведения, правовых гарантий и т.п. выглядит нонсенсом.

При этом интуитивно большинство юристов осознают, что идеальная модель права очень сильно отличается от реальности. Ведь есть мертворожденные нормы, то есть те, которые никогда не применялись в силу фактической невозможности их применения. К ним относится, например, порядок учета средств цветного копирования, предусматривающий их обязательную регистрацию: он был установлен в 1994 году [10] и отменен только в 2010 [11]. Регистрации подлежали средства цветного копирования (оперативной полиграфии, копировально-множительной техники, капельно-струйных принтеров), приобретаемые гражданами, а также предприятиями, организациями и учреждениями независимо от форм собственности и сферы деятельности (далее именуются - предприятия). Утвержденные Правила предусматривали, что граждане и руководители (представители) предприятий обязаны в течение месяца со дня приобретения средств цветного копирования представить в орган внутренних дел соответственно по месту жительства или по месту нахождения предприятия либо по месту использования средств цветного копирования паспорт либо иной документ,

удостоверяющий их личность или служебное положение (полномочия), а также письменное заявление произвольной формы о регистрации указанных средств. Орган внутренних дел обязан в течение месяца со дня обращения граждан или предприятий произвести обследование помещения, предназначенного для хранения и использования средств цветного копирования, в целях определения его соответствия требованиям, установленным настоящим пунктом, и принять решение о регистрации указанных средств. Помещение, предназначенное для хранения и использования средств цветного копирования, должно быть изолированным от других помещений, технически укреплено от проникновения посторонних лиц (охранной сигнализацией, надежными запорами и т. п.), чтобы исключить возможность бесконтрольного использования этих средств.

Еще один пример отличия «идеального» права от реальности – судебные решения, иногда весьма вольно трактующие положения правовых актов; при этом суды, даже Конституционный Суд Российской Федерации, могут менять свою трактовку одних и тех же положений. Как отмечал в своем интервью В.Д. Зорькин, «живая Конституция – это не только текст и не только решения КС по толкованию тех или иных норм Основного закона. Живая Конституция – это еще и законы, и вся правоприменительная практика, которая показывает, в каком направлении двигается наше право. Ядром этой практики является, конечно, конституционное правосудие. То есть важен не только сам текст Конституции, но и его реальное воплощение в жизнь. И важны не только учреждения, которые там названы, а то, как эти парламент, президент, суды, СМИ функционируют. Важен не столько перечень прав и свобод, сколько то, как они реализуются. Согласитесь, любой текст можно озвучить так, что все хорошее в нем будет перечеркнуто» [12]. Наконец, существует практика надзорных органов, которые могут применять или не применять отдельные предписания законов и подзаконных актов.

Однако позитивистские устои не позволяют признать, что право (как минимум – писаное право) имманентно несовершенно. Отсюда – постоянные заклинания о «необходимости совершенствования законодательства» как средстве решения проблем. Но законодательство, да и право в целом несовершенны всегда! Расхождение между писаным правом и фактически применяющимися в обществе правилами поведения подтверждалось исследователями и в XIX веке, и в XXI: можно вспомнить и концепцию «фактической конституции» Ф. Лассаля, и «живое право союзов» Е. Эрлиха. Соотношение закона и его использования в обществе является предметом и современных социологических исследований [13].

Разумеется, нельзя пытаться ставить под сомнение авторитет законодательства, подрывать общеобязательность правовых норм и необходимость их применения. Как отмечал И.А. Покровский, «как в области публичного, так и в области гражданского права залогом истинного праворазвития может быть только одно – законность и правовой порядок». Радикальное же расхождение законов и представлений общества о справедливости свидетельствует о кризисе в обществе и запросу к власти на модернизацию [14, с.223]. Тем не менее, надо обратить внимание, что имманентная несовершенность права – даже в том обществе, где право воспринимается населением как справедливое – имеет объективные предпосылки, выступающие пределами права, точнее - пределами правового регулирования.

Для того, чтобы рассмотреть пределы правового регулирования, придется отойти от позитивистских устоев. Конечно, в конкретном месте и в конкретный момент времени и государство, и право выступают в виде объективной реальности, не зависящей от конкретного человека. Так, сейчас мы живем в Российском государстве, основой правовой системы которого является Конституция Российской Федерации. Однако даже в истории нашего народа было несколько моментов, когда и государство, и право этого государства

разом переставали существовать: это происходило с СССР [15], и с Российской Империей [16]. В зарубежной истории это случалось еще чаще; зачастую даже нельзя было с определенностью сказать, существует государство или нет – например, в Ливии. Право может существовать без государства, как это было с римским правом. Некоторые члены общества могут не признавать право соответствующего государства – тогда оно не будет для них правом (примеры такого поведения можно видеть в некоторых национальных общностях и в террористических организациях; самым же красивым «мысленным экспериментом» такого рода является Воланд и его свита в «Мастере и Маргарите» М.Н. Булгакова: хотя они находятся на территории Советского государства, и на них распространяется действие советских законов, они не считают необходимым им подчиняться – и заставить их подчиниться нет никакой возможности). Поэтому право и государство для целей нашего исследования – это то, что признается правом и государством в конкретном обществе в конкретный момент времени. Государство при этом выступает в качестве механизма принятия общеобязательных решений в обществе, а право – накопленной и распространяемой в обществе информацией о таких решениях. Чем же будет ограничиваться использование данных инструментов, то есть что будет выступать пределами правового регулирования? Вопрос этот тем более важен, что право как инструмент регулирования в обществе нужно использовать экономно, не тратя на это ограниченные ресурсы самого общества. Можно написать закон, который выйдет за пределы правового регулирования, потратить существенные правоприменительные ресурсы в попытке его реализовать – но все равно потерпеть неудачу. Недаром ведь В.А. Дозорцев писал, что «право основано на объективных закономерностях, нарушение которых раньше или позже жестоко мстит за себя» [17, с.228].

Можно выделить две группы пределов правового регулирования (в достаточно общем понимании этого термина как, скажем, «границы государственного вмешательства в систему общественных отношений» [18]): внутренние, обусловленные собственными характеристиками права, и внешние, обусловленные взаимодействием права с обществом.

Первый внутренний предел правового регулирования связан с тем, что нормы права рассчитаны на многократное применение и упорядочивание на этой основе общественных отношений. Даже в учебниках по основам права отмечается, что «при помощи общих правил достигается единый действующий порядок во взаимоотношениях людей в обществе, снижаются возможности для индивидуального произвола. Свои отрицательные моменты имеет и нормативное регулирование, в особенности в случаях, когда требуется учет неповторимой специфики определенной ситуации» [19, с.22]. Правовое регулирование достигает своего предела в силу того, что жизнь богаче и разнообразнее любого, даже самого продуманного закона. Объективным основанием для данного предела выступают законы математической статистики, связанные с распределением вероятностей. Математически доказано, что вероятность развития событий по тому или иному варианту распределяется некоторым образом: какие-то случаются чаще, какие-то реже. Любая общая норма «накрывает» только часть вариантов, пусть и самую вероятную. Остальные варианты этой нормой отсекаются – либо как противоправные, либо как «непредусмотренные».

Именно об этом пределе писал В.П. Грибанов: «соотношение между поведением, составляющим содержание субъективного права, и поведением, составляющим содержание осуществления права, представляется прежде всего как соотношение между возможностью и действительностью. … поведение, составляющее процесс осуществления права, всегда есть определенный, конкретный вид реальных действий управомоченного лица, вытекающий из особенностей данного конкретного случая. Поэтому соотношение между поведением, составляющим содержание субъективного права, и поведением, составляющим содержание процесса его осуществления, представляется так же, как соотношение общего и конкретного, как соотношение общего типа поведения и

конкретных форм его проявления в условиях данного конкретного случая» [20, с.44-45]. Самый мудрый законодатель не в состоянии при написании общей нормы помыслить все те внешние обстоятельства, в которых будет складываться правоотношение; норма, таким образом, оказывается на эти обстоятельства не рассчитана.

Показательным случаем достижения правом данного предела является злоупотребление правом – одна из «неразрешимых проблем» правовой науки. Как справедливо отмечает А.В. Волков, «злоупотребление правом - это всегда проявление системного «сбоя» норм в гражданском праве; когда их использование в ситуации правовой неопределенности производится не по назначению; нормы (а точнее их формализм и несовершенство) становятся средством злоупотреблений» [21]. Случаи обхода закона, о которых говорится в пункте 1 статьи 10 Гражданского кодекса РФ (далее – ГК РФ) – также яркий пример достижения правовым регулированием своего предела.

Так как данный предел носит объективный характер и с неизбежностью присущ правовому регулированию, нет никакой возможности разрешить данный кризис правовыми средствами. Существует два способа сглаживания кризиса: введение «каучуковых норм» (запрета злоупотребления правом, запрета недобросовестного поведения и т.п.) и уточнение самой правовой нормы. И то, и другое не позволяет решить проблему полностью, так как, опять-таки, не может учесть все возможные жизненные обстоятельства. Кроме того, активное использование обоих способов само по себе влечет пагубные последствия. Широкое применение каучуковых норм нарушает определенность права, на что указывал еще И.А. Покровский [16, с.220]. Попытка же учесть в общей норме все возможные частные случаи затрудняет восприятие этой нормы (вспомним Налоговый кодекс РФ) – и это угрожает достижением второго внутреннего предела правового регулирования.

Второй предел правового регулирования связан с познаваемостью права. Как уже говорилось выше, право – это прежде всего информация, соответственно, его надо соотносить с когнитивными возможностями человека. Об этом давно уже говорят социологи: «В России плотность правил как в Германии, а качество — как в Гане. Очень плохие законы, при этом их очень много. Обычно там, где не умеют писать законы, их и немного, а там, где умеют, накручивают много-много правил — люди стонут от бюрократии, но и правила не противоречат друг другу. В России люди окружены огромным количеством мелочных правил, и следовать им всем невозможно. Они противоречат друг другу, за ними не уследишь, они все время меняются. Что людям остается? Придумать какие-то причины, почему их нарушать оптом. Вот это объективная, рациональная составляющая» [22].

Познаваемость права является важнейшим фактором, впрочем, давно осознанным юристами. Те правила, от которых зависит жизнь и здоровье людей – например, Правила дорожного движения – постарались сделать максимально наглядными. Главное юридическое изобретение XX века – светофор – является образцом доступного для познавания правила поведения, что и предопределяет его эффективность и всемирное распространение. Другой пример: типовые лицензии Creative Commons, позволившие сделать прорыв в адаптации авторского права к реалиям Интернета. Эти лицензии изложены на трех уровнях: юридическом, «для обычного человека» и машиночитаемом. Уровень «для обычного человека» позволяет буквально за несколько секунд понять, какие возможности предоставляются текстом лицензии, и сделать выбор. При этом существует полноценный юридический текст, учитывающий наиболее распространенные обстоятельства, в которых может складываться правоотношение, урегулированное лицензией. Во многом ориентация на когнитивные способности адресата правовой нормы предопределила успех Единого портала государственных и муниципальных услуг (gosuslugi.ru). При наполнении данного веб-сайта была проведена огромная работа по

структурированию требований к получателям услуг, изложению этих требований в доступной и наглядной форме.

Социологи отмечают, что «в России очень плохо пишутся законы, и по мере ужесточения режима они пишутся все хуже, потому что нет обратной связи. Правила пишутся от балды. Нет дискуссий, нет диалога, нет площадки для обсуждения. В последнее время уже и ведомственных экспертов не спрашивают, когда пишут законы, про независимых-то давно забыли. И получается, что даже в отсутствие злонамеренности просто не удается просчитать, какие проблемы возникнут, если очередное правило будет введено»[22]. С этим утверждением можно согласиться лишь отчасти: есть дискуссия, есть взаимодействие с экспертами. Но самые важные законопроекты принимаются в трех чтениях за неделю – неудивительно, что написанные таким образом нормы трудно укладываются в головах тех, кому они адресованы. Причину такого волюнтаризма хорошо описал С.С. Алексеев: «главным в жизни является реально существующая в данный момент доминирующая сила (власть), способная оперативно и эффективно принимать решения, необходимые для общества потребления, запрещать, приказывать и дозволять. Притом такие решения по схемам «ручного управления», которые при необходимости должны иметь незамедлительный и действенный характер. Такой силой по многовековой традиции стала трактоваться верховная государственная власть (такую же функцию обрели подчиненные верховной власти спецслужбы)» [7, с.20].

Следовательно, можно констатировать, что быстрому достижению правовым регулированием своего второго предела, способствует отсутствие обязательной для законодателя обратной связи. Без этого право превращается в свою противоположность – в произвол, и перестает быть правом. Наличие второго предела права требует наличия конкуренции – политической и общественной – при формулировании правовых норм, поскольку, как показывает практика, только она позволяет формулировать правовые нормы, отвечающие когнитивным возможностям субъектов: познаваемость норм многократно проверяется еще на стадии их разработки. Здесь работают те же законы, что и в рыночной экономике: конкуренция, невидимая рука рынка, а фактически – само человечество как самый мощный из доступных нам вычислительных ресурсов эффективно ограничивают взаимные интересы субъектов, позволяя найти пусть даже не самое эффективное, но хотя бы понятное решение и закрепить его в правовой норме. Так называемое lex informatica [24, с. 553-593], «право как код», то есть правовые нормы, подкрепленные обеспечивающими их исполнение информационными технологиями, тоже дает сильнейший эффект обратной связи, выступая своего рода «сывороткой правды» для законодателя. В этом случае не качество законов обеспечивает их надлежащее выполнение, а наоборот, неизбежность выполнения законов (в силу невозможности обойти технологию) ставит особые требования к качеству закона.

Перейдем к внешним пределам правового регулирования. Первым из них выступает достаточно хорошо раскрытый в литературе территориальный предел (действие закона в пространстве и по кругу лиц). Как указывает А.А. Тилле, принцип территориального действия законов самым плотным образом связан с принципом суверенитета: «власть государства ограничена его территориальными пределами (границами) и действие его велений (законов) не выходит за эти пределы» [25, с.104]. Экстерриториальное действие закона (то есть применение его вне пределов юрисдикции данного государства) возможно, но является, скорее, исключением, требующим в большинстве случаев согласия того государства, на территории которого применяется норма (например, путем применения судом иностранного права).

Вопрос о территориальном пределе правового регулирования с новой силой стал обсуждаться по мере развития интернета. Уже в ранних исследованиях по тематике права и интернета проблемы юрисдикции, коллизионного права, экстерриториального действия законов получили центральное место [26, с.10; 27, с.66; 28, с.14]. С подписанием

Конвенции о преступности в сфере компьютерной информации ETS N 185 (Будапешт, 23 ноября 2001 г.), предусматривающей право на преследование нарушителя на виртуальной «территории» другого государства, разоблачениями Э. Сноудена, появлением в российском законодательстве института «организатора распространения информации» вопрос об интернете как «новой территории» приобрел еще большую актуальность. Поскольку возможные пути решения данной проблемы были рассмотрены ранее [29], хотелось бы отметить наличие «встроенного» механизма обратной связи в данном пределе правового регулирования. Поскольку право, как отмечалось выше, обеспечивается государственным принуждением, экстерриториальное действие закона также возможно только в тех случаях, когда государство сможет обеспечить принудительное осуществление норм своего права в другом государстве. Можно сколько угодно пытаться распространить действие российских законов на американские компании, но принудительно реализовать соответствующие нормы возможно только в случае, когда эти компании участвуют в отношениях с российскими организациями или гражданами. В то же время, территориальный предел правового регулирования достаточно гибок, поскольку право всегда следует за общественными отношениями, которые оно регулирует. Общественные отношения выступают «ниточками», за которые можно аккуратно притянуть ту или иную область деятельности в мире или в регионе под юрисдикцию сильного государства. Это происходит с персональными данными в силу Конвенции Совета Европы ETS N 108, с финансовой информацией в силу FATCA – примеров можно привести множество. Достижение и преодоление территориального предела правового регулирования, таким образом, является прямым следствием неуспешности или успешности внешней политики того или иного государства.

Вторым внешним пределом правового регулирования выступает неприкосновенность частной жизни. Связано это с тем, что за последние несколько десятков лет акцент в правовой охране частной жизни сместился с неприкосновенности на право контролировать информацию о себе. Эту трансформацию убедительно показывает Stefano Rodotá, просто перечисляя определения privacy разных лет: Warren and Brandeis – “the right to be left alone” (1890-e) и A. Westin - “the right to control the way others use the information concerning us” (1970-e). Впрочем, сам данный исследователь придерживается дуалистического понятия privacy, определяя ее как “the right to keep control over one’s own information and determine the manner of building up one’s own private sphere” [30, с.78-79]. В отечественном же законодательстве подходы «неприкосновенности» и «контроля» и вовсе смешались: регулирование отдельных видов отношений, прежде всего - обработки персональных данных обосновывается необходимостью защиты прав на неприкосновенность частной жизни, личную и семейную тайну [31, с.2]. Однако – и это подчеркивается некоторыми исследователями - персональные данные и неприкосновенность частной жизни суть разные правовые категории [32]. На том же тезисе основывается и позиция Конституционного Суда Российской Федерации: «В понятие «частная жизнь» включается та область жизнедеятельности человека, которая относится к отдельному лицу, касается только его и не подлежит контролю со стороны общества и государства, если она носит непротивоправный характер» [33]. Неприкосновенность частной жизни, таким образом, необходимо расценивать в качестве предела правового регулирования, за которым право теряет свою силу.

В пользу наличия данного предела можно выдвинуть две группы аргументов: одни относятся к тому, что право не должно вторгаться в частную жизнь, другие – что право фактически не может регулировать частную жизнь. Аргументы первой группы использовались с конца XIX века при формировании самого института приватности (privacy), института неприкосновенности частной жизни. Знаменитая работа Воррена и Брандейса, которой был введен в научный оборот сам термин «приватность» (privacy) опиралась на сформировавшуюся к тому времени в судебной практике доктрину «права

быть оставленным в покое» – "right to be left alone". Область частной и домашней жизни названа авторами священной, а любое посягательство на нее должно быть пресечено [34, с.195]. В этом же ключе понимается частная жизнь в базовых документах по правам человека:

- статье 12 Всеобщей декларации прав человека 1948 года («Никто не может подвергаться произвольному вмешательству в его личную и семейную жизнь, произвольным посягательствам на неприкосновенность его жилища, тайну его корреспонденции или на его честь и репутацию. Каждый человек имеет право на защиту закона от такого вмешательства или таких посягательств»);
- статье 8 Европейской конвенции по правам человека 1950 года («Каждый имеет право на уважение его личной и семейной жизни, его жилища и его корреспонденции»).

Как уже указывалось выше, схожим образом – как сфера, не подлежащая контролю со стороны общества и государства – понимается частная жизнь и Конституционным Судом Российской Федерации.

Аргументы в пользу того, что право не только не должно, но и не может регулировать частную жизнь, наиболее явно были обозначены в споре о так называемом частном использовании интеллектуальной собственности (прежде всего, копировании произведений в личных целях). А.Ю. Кувыркова, рассматривая историю данного вопроса, отмечает: «Ряд зарубежных авторов настаивают на том, что совпадение области, защищаемой правом на неприкосновенность частной жизни, и области, находящейся за пределами законодательства об интеллектуальной собственности, не является случайностью, а соображения неприкосновенности частной жизни лежат в основе современного законодательства об авторском праве и смежных правах и будут вставать на пути любых попыток осуществления исключительных прав в отношении использования объектов в личных целях. Соглашаясь с доводами указанных авторов, нельзя не признать, что указанное ограничение действия исключительных прав существуют все же, скорее, благодаря экономической нецелесообразности и практической невозможности контроля над частным использованием, нежели благодаря принципиальной позиции законодателя» [35, с.47]. Нельзя не вспомнить и эпохальное решение Bundesverfassungsgericht (один из судов ФРГ) 1983 года, который фактически признал невозможность обязать владельцев копировальных салонов контролировать каждую копию, изготавливаемую своими клиентами, не только потому, что подобный контроль нарушал бы право на неприкосновенность частной жизни, предоставленное Основным законом ФРГ, но и потому, что такой контроль практически невозможен [36; 35, с.46-47; 30, с.79]. Надо отметить, что интересы правообладателей при этом не пострадали: достигнув своего предела, правовое регулирование было направлено в другое русло, в результате чего появился сбор с производителей копировального и звукозаписывающего оборудования в пользу организаций по управлению правами на коллективной основе.

Безусловно, современные информационные технологии соблазняют возможностью выйти за данный предел правового регулирования, вторгнувшись в частную жизнь, и законодатель зачастую идет на поводу у этого соблазна. Наступление на частную жизнь идет в сфере авторского права и смежных прав: последовательно были добавлены статьи про технические средства защиты авторского права и смежных прав (статья 48.1 Закона РФ от 9 июля 1993 г. N 5351-I «Об авторском праве и смежных правах»), потом из пункта 3 статьи 1299 ГК РФ было убрано упоминание о том, что технические средства защиты авторского права ограничиваются случаями свободного использования произведений, затем были ограничены и сами случаи свободного использования в личных целях (пункт 1 статьи 1273 ГК РФ). Все эти поправки дали правообладателю неограниченную

возможность контролировать частное использование путем внедрения технических средств защиты авторского права, неизбежных для пользователя. Вторжение в частную жизнь идет и в области публичного права: поправки [37; 38] в Федеральные законы от 07.07.2003 № 126-ФЗ «О связи» и от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» установили обязанность операторов связи и организаторов распространения информации хранить содержание сообщений своих пользователей.

Однако практика показывает неэффективность любых попыток регулирования частной жизни. Как было показано ранее [39], те компании, которые не пытаются контролировать частное использование, получают конкурентное преимущество на рынке. Нет смысла бороться с собственными пользователями. В этом и заключается смысл неприкосновенности частной жизни как предела правового регулирования: любые попытки выйти за него являются неоправданными; при этом, как правило, существует решение проблемы, не связанное с выходом за данный предел правового регулирования (например, сбор с производителей оборудования в случае с частным использованием произведений).

Зарубежная доктрина демонстрирует возврат к разделению категорий «неприкосновенности» и «контроля» применительно к частной жизни, которые, как рассматривалось выше, неоправданно смешались в 1970-90-е годы. Так, в Статуте фундаментальных прав ЕС [40] были разделены Статья 7, посвященная праву на уважение к частной и семейной жизни, и Статья 8, посвященная праву на защиту персональных данных (т.е. данных, относящихся к этому человеку). С. Родота, анализируя данные положения Статута, отмечает принципиальную разницу в данных категориях: право на уважение к частной жизни – это «статическое» право, право с отрицательным содержанием, действующее «против всех» и защищающее от вторжений. Право на персональные данные – это право «динамическое», побуждающее к собственным действиям субъекта, и следующее не за субъектом, а за данными о нем, его «цифровым» образом. «Мы сталкиваемся с заново изобретенной защитой персональных данных – не только потому, что она создает самостоятельное фундаментальное право, но и потому, что она является эффективным инструментом для развития индивидом собственной личности» [30, с.80]. К этому можно добавить и то, что право контролировать данные о себе, о котором часто говорится в литературе, не является обязанностью контролировать такие данные, и в том числе поэтому здесь требуется публично-правовая охрана. В одном случае она будет защищать от вторжения в частную жизнь, в другом - предотвращать незаконное использование персональных данных в общественных отношениях.

В рамках своих пределов правовое регулирование является уникальным инструментом, позволяющим упорядочивать общественные отношения. Конечно, нельзя забывать и про наличие системы государственного принуждения как фактора эффективности правового регулирования. Однако она вступает в действие только в тех случаях, когда правовое регулирование используется как инструмент изменения общественных отношений, а не как инструмент фиксации сложившихся в обществе отношений. Понимание этого момента крайне важно в целях экономного использования ресурсов государства, ресурсов аппарата принуждения. Во многих юридических работах используется красивое словосочетание «поиск баланса». Е.А. Войниканис в своей работе [41] указывает на множество исследований и правовых актов, где упоминается необходимость поиска баланса интересов, и даже говорит о принципе баланса интересов применительно к праву интеллектуальной собственности. Так вот, экономия государственного принуждения требует, чтобы право не «искало баланс» интересов, заставляя общественные отношения изменяться против воли их участников, а лишь фиксировало тот баланс интересов, который уже сложился в обществе, который понят и принят участниками отношений. «Правопреобразующая» функция может использоваться

лишь тогда, когда принято решение о реформе, изменении отживших свое или неэффективных отношений. Общество в большинстве случаев способно само найти такой баланс в силу состояния конкуренции, когда интересы сторон взаимно ограничиваются самостоятельными действиями каждой из них. «Поиск баланса» средствами правового регулирования необходим только тогда, когда конкуренция отсутствует, то есть одна из сторон правоотношения является слабой и не может эффективно отстаивать свои интересы (в экономическом анализе права такие ситуации описываются как market failure, сбои конкурентного механизма, требующие, как минимум, в среднесрочной перспективе, вмешательства государства.). Однако и в этом случае цель правового регулирования должна заключаться в том, чтобы запустить рыночные, конкурентные механизмы защиты субъектами своих интересов – прежде всего, на основе информационных технологий, устраняющих транзакционные издержки. Наличие таких рыночных, конкурентных механизмов позволит не тратить ресурсы государства по поддержанию баланса интересов.

ЛИТЕРАТУРА

1. Морозова Л.А. Теория государства и права: Учебник. М., 2002.

2. Общая теория государства и права. Академический курс в 2 томах. Под ред. М.Н. Марченко. Т.2. М., 1998.

3. Ленин В.И. Полное собрание сочинений (5-е издание). Москва: Издательство политической литературы, 1965-75. Т.2.

4. Алексеев С.С. О понятии права // «Правоведение», 1970, №1.

5. Братусь С.Н. Юридическая ответственность и законность: очерк теории. М., 1976.

6. Рабинович П.М. Право как веление общественного сознания. «Правоведение», 1972, №2.

7. Алексеев С.С. Крушение права. Полемические заметки. Екатеринбург, 2009.

8. Zherebtsov Mikhail. President Putin’s Conception of the Rule of Law // Journal of parliamentary and political law [8 J.P.P.L.].

9. Емельянов В. Запрет злоупотребления гражданскими правами. // «Законность», 1999, №10.

10. Постановление Правительства РФ от 11 октября 1994 г. № 1158 «О порядке учета, хранения и использования средств цветного копирования в Российской Федерации».

11. Постановление Правительства РФ от 29 июля 2010 г. № 580.

12. Интернет-интервью с В.Д. Зорькиным, Председателем Конституционного Суда РФ. URL: http://www.consultant.ru/law/interview/zorkinbd/ (дата обращения 01.07.2018)

13. Петрова Н. Справедливость в порядке очереди. URL http://kommersant.ru/doc/2944658 (дата обращения 01.07.2018).

14. Покровский И.А. Гражданский суд и закон. Проблема их взаимоотношения // Вестник гражданского права, 2009, №1, т.9.

15. Соглашение о создании Содружества Независимых Государств (Минск, 8 декабря 1991 г.).

16. Положение о народном суде, утвержденное Декретом ВЦИК от 30 ноября 1918 года.

17. Дозорцев В.А. Принципиальные черты права собственности в гражданском кодексе // Гражданский кодекс России. Проблемы. Теория. Практика: Сборник памяти С.А. Хохлова / отв. ред. А.Л. Маковский; М.: Родос, 1998.

18. Абросимова Е.А. Российский некоммерческий сектор: пределы правового регулирования // Сборник научно-практических статей III-ей Международной научно-практической конференции «Актуальные проблемы предпринимательского и корпоративного права в России и за рубежом» (25 апреля 2016 года, г. Москва) (под общ. ред. С.Д. Могилевского, М.А. Егоровой) М., 2016.

19. Власов В.И., Низовцев В.В., Шевченко В.Л. Основы правоведения: учебное пособие для студентов неюридических специальностей. Ростов-на-Дону, 1997.

20. Грибанов В.П. Осуществление и защита гражданских прав. М., 2001.

21. Волков А.В. Принцип недопустимости злоупотребления гражданскими правами в законодательстве и судебной практике (Анализ более 250 судебных дел о злоупотреблении правом). Специально для системы ГАРАНТ, 2012.

22. Интервью Эллы Панеях изданию «Медуза» URL https://meduza.io/feature/2016/02/19/v-rossii-gosudarstvo-namnogo-huzhe-naseleniya (дата обращения 01.07.2018).

23. С. Кучер. Интервью с Далай-Ламой XIV // Газета «Коммерсантъ» №149 от 16.08.2017, с.6.

24. Reidenberg, Joel R. Lex Informatica: The Formulation of Information Policy Rules Through Technology // Texas Law Review Volume 76, Number 3, February 1998.

25. Тилле А.А. Время, пространство, закон. М., 1965.

26. Кемрадж А.С. К вопросу об юрисдикции государства в отношении отдельных сегментов сети Интернет / Правовые аспекты использования интернет-технологий. М., 2002.

27. Якушев М.А. Интернет и право // «Законодательство», 1997, №1.

28. Малахов С.В. Гражданско-правовое регулирование отношений в глобальной компьютерной сети Интернет. Автореф. дисс… канд. юрид. наук. М., 2001.

29. Дмитрик Н. Единый и неделимый? Как уберечь глобальный интернет от национального дробления. URL: https://digital.report/global-vs-national-internet/ (дата обращения 01.07.2018)

30. Rodotá S. Data Protection as a Fundamental Right // Reinventing Data Protection? Springer Science+Business Media B.V. 2009.

31. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

32. Войниканис Е.А., Машукова Е.О., Степанов-Егиянц В.Г. Неприкосновенность частной жизни, персональные данные и ответственность за незаконные сбор и распространение сведений о частной жизни и персональных данных: проблемы совершенствования законодательства // «Законодательство», 2014, № 12.

33. Определение Конституционного Суда РФ от 9 июня 2005 г. N 248-О «Об отказе в принятии к рассмотрению жалобы граждан Захаркина Валерия Алексеевича и Захаркиной Ирины Николаевны на нарушение их конституционных прав пунктом «б» части третьей статьи 125 и частью третьей статьи 127 Уголовно-исполнительного кодекса Российской Федерации»

34. Warren S.D., Brandeis L.D. The Right to Privacy. Harvard Law Review, 1890, 4.

35. Кувыркова А.Ю. Осуществление исключительных интеллектуальных смежных прав. Дисс. … канд. юр. наук. М., 2010

36. Kopierläden, German Federal Supreme Court, 9 June 1983, GRUR 54.

37. Федеральный закон от 5 мая 2014 г. № 97-ФЗ

38. Федеральный закон от 6 июля 2016 г. № 374-ФЗ.

39. Дмитрик Н. Пират дома: как бороться с цифровым пиратством. URL: https://digital.report/pirat-doma-kak-borotsya-s-tsifrovyim-piratstvom/ (дата обращения 01.07.2018)

40. Charter of Fundamental Rights of the European Union. URL: www.europarl.europa.eu/charter/pdf/text_en.pdf (дата обращения 01.07.2018).

41. Войниканис Е.А. Право интеллектуальной собственности в цифровую эпоху: парадигма баланса и гибкости. М., 2013.

3. ПРАВА НА ИНФОРМАЦИЮ, НЕПОСРЕДСТВЕННО СВЯЗАННУЮ С ЛИЧНОСТЬЮ ФИЗИЧЕСКОГО ЛИЦА, И ИНЫЕ ПРАВА НА ИНФОРМАЦИЮ

Права на информацию и права доступа к информации в информационных системах и ресурсах являются субъективными правами, принадлежащими гражданам, их объединениям, юридическим лицам и публичным субъектам (государствам и их органам). Для того, чтобы проанализировать права на информацию и права на доступ к информации, необходимо кратко описать понятие субъективного права, установить его содержание и провести классификацию прав по основаниям, имеющим значение для целей настоящего исследования.

Под субъективным правом в литературе, как правило, понимается мера возможного поведения управомоченного лица, юридическая мера свободы человека [1, с.254]. Осуществлением субъективного права является поведение управомоченного лица, реализующее меру свободы, заложенную в содержании права [2, с.294.]. Субъективное право необходимо рассматривать как модель поведения. Функциональные характеристики этой модели обусловливаются содержанием субъективного права. Осуществление же права есть практический, реальный процесс, который и был описан в идеальной правовой модели.

Для целей настоящего исследования принципиально важной является характеристика субъективного права именно как возможного, а не только лишь дозволенного поведения. Данный аспект субъективного права до настоящего времени не имеет устоявшегося понимания в юридической науке. С одной стороны, определение права через возможность мало что дает по сравнению с дозволенностью: «То, что дозволено, то и юридически обеспечено» [3, с.11]. С другой стороны, субъективное гражданское право – не только дозволенность, но еще и возможность, возникающая вследствие обеспечения определенного поведения обязанных лиц. «Для государства предоставление прав различным субъектам имеет значение постольку, поскольку оно обеспечивает такое поведение обязанных лиц, которое установлено государством в качестве обязательного при данных обстоятельствах. Для управомоченного наделение его субъективными правами значимо постольку, поскольку оно обеспечивает такое поведение других лиц, которое необходимо управомоченному при данных условиях» [4, с.216]. Для целей настоящей работы необходимо включить в понятие субъективного права оба признака: «субъективное право – это дозволенная законом мера возможного поведения управомоченного лица» [2, с.292]. Возможность осуществления определенных действий необходимо анализировать, прежде всего, как их дозволенность, т.е. с позиций границ субъективного права, установленных действующим законодательством. «Всякое

субъективное право, будучи мерой возможного поведения управомоченного лица, имеет определенные границы как по своему содержанию, так и по характеру его осуществления. <…> Границы есть неотъемлемое свойство всякого субъективного права, ибо при отсутствии таких границ право превращается в свою противоположность – в произвол и тем самым вообще перестает быть правом» [2, с. 22]. Таким образом, необходимо сделать особый упор на вопросы реальной осуществимости тех идеальных моделей поведения, которые заложены в правовой норме. В этом ключе – как реальные возможности поведения в рамках установленной законом модели – права на информацию и права на доступ к информации рассматриваются в настоящем исследовании.

Говоря о содержании права на информацию и о классификации таких прав, важно выделение абсолютных и относительных прав на информацию. По общему правилу, различение абсолютных и относительных прав основывается на различии в круге обязанных лиц, противостоящих лицу, обладающему правом. «Абсолютными считаются те права, где управомоченному лицу противостоит неопределенный круг обязанных лиц. Таково, например, право собственности, право авторства на произведение науки и т. п. Как собственнику, так и автору противостоят все другие лица, на которых лежит обязанность не препятствовать осуществлению права, не нарушать прав этих лиц. Относительными признаются такие гражданские права, где управомоченному лицу противостоит определенный круг обязанных лиц. В относительных правоотношениях на обязанной стороне может быть как одно лицо, так и несколько лиц, но круг обязанных лиц всегда точно известен» [2, с.294].

По результатам исследования можно сделать вывод о том, что в странах ЕАЭС отсутствует абсолютное право на информацию как таковую. При этом в законодательстве отдельных стран сохранены рудименты такого права в виде «права собственности» на информацию, составляющую государственную или служебную тайну [7, ст.3; 8, ст.1], однако на практике этот режим не применяется. Также в законодательствах стран ЕАЭС предусмотрены, как будет показано далее, разные виды исключительного права на информацию, представленную в форме отдельных результатов интеллектуальной деятельности.

С точки зрения осуществления прав важным является то, что в абсолютных правоотношениях управомоченному лицу противостоят лишь пассивно обязанные лица, в то время как в обязательственных правоотношениях на другой стороне есть одно или несколько лиц, на которых может быть возложена обязанность активного типа. Хотя это и не означает, что в обязательственных правоотношениях нет круга лиц, обязанных воздерживаться от нарушения чужого права, наличие конкретного позитивно обязанного лица принципиально важно для характеристики отношений именно в качестве обязательственных. «Иначе говоря, будучи прямой в отношении абсолютных прав, всеобщая пассивная обязанность является косвенной в отношении прав относительных» [4, с.624-625]. В виде относительных прав закреплены в законодательствах стран ЕАЭС различные виды прав, относящихся к доступу к информации. К ним можно отнести как право уполномоченных государственных органов (например, налоговых) на получение данных из информационных ресурсов и систем, так и право граждан на получение информации о деятельности государственных органов, установленное законодательством о доступе граждан к такой информации [9, 10]. Во всех случаях субъективному праву лица на доступ к информации корреспондирует обязанность обладателя информации ее предоставить.

Различию отношений абсолютных и относительных корреспондирует различие способов, которыми могут осуществляться права и исполняться обязанности в этих отношениях. Субъективное право в абсолютных отношениях осуществляется, как правило, «статическими» способами (фактическим пользованием имуществом), собственными действиями управомоченного субъекта. «Появление лиц, активно

обязанных перед собственником, свидетельствует либо о том, что отношения собственности находятся в аномальном состоянии, либо о том, что на их основе возникли новые правоотношения, - обязательственного, трудового или иного характера, - выходящие за пределы юридических отношений собственности» [4, с.617]. Напротив, в относительных правоотношениях субъективное право осуществляется путем обращения требований к обязанной стороне. При этом на самом управомоченном лице, как правило, лежат определенные обязанности.

Способы исполнения обязанностей в абсолютных и относительных правоотношениях также различаются. Характерные для абсолютных правоотношений обязанности пассивного типа исполняются путем соблюдения установленных в законе запретов. Обязанности активного типа могут существовать только в относительных правоотношениях; они исполняются активными действиями обязанного субъекта, которые рассматриваются законом или договором в качестве юридического факта, влекущего возникновение, изменение или прекращение правоотношений.

Как уже было отмечено выше, в странах ЕАЭС отсутствует абсолютное право на информацию, соответствующее всем рассмотренным выше признакам абсолютного права. Однако можно заметить, что в законодательстве стран ЕАЭС имеются права в отношении информации, обладающие отдельными признаками абсолютных прав. Такие права можно рассматривать как «ослабленные абсолютные». К ним относится, например, исключительное право, а также некоторые права, связанные с возможностью контролировать последующее использование информации, полученной из определенного источника (например, право контролировать последующее распространение информации, составляющей государственные секреты, банковскую тайну, налоговую тайну).

Ослабленные абсолютные права не устанавливают конкретной связи между двумя лицами (как относительные), а обращены к неопределенному кругу обязанных лиц, но их особенность заключается в том, что этот круг обязанных лиц все-таки может быть ограничен» [5, с.120]. Специфика информации как объекта прав, то есть его нематериальный характер, определяет ряд особенностей исключительных прав по сравнению с правом собственности (классическим абсолютным правом).

Во-первых, необходимым условием установления абсолютного права на объект является обособление данного объекта от других, сходных с ним или являющихся по отношению к нему производным или исходным объектами. Такая задача не стоит перед правом собственности, где объектом всегда является вещь, то есть предмет материального мира, имеющий материальные же границы в пространстве.

Во-вторых, поскольку материальный объект ограничен в пространстве и может «применяться» в определенный момент только одним лицом или ограниченным кругом лиц, а нематериальный объект может быть использован одновременно неопределенным кругом лиц, классические для абсолютного права правомочия владения, пользования и распоряжения объектом права должны быть трансформированы. Право на интеллектуальный продукт «не включает и не может включать в себя право владения, которое всегда имеет своим объектом материальную вещь, его нет вовсе. Другое содержание по сравнению с пользованием по праву собственности имеет право использования интеллектуального продукта; отличается и понятие распоряжения. … Использование основано на другом по сравнению с пользованием по праву собственности принципе – на необходимости специального установления запрета для третьих лиц в каждом отдельном случае, а при его отсутствии – в свободе использования. Особенности использования обусловливают и специфическое содержание права распоряжения, которое должно позволять передачу объекта для использования не только одному лицу (передачу права), но и предоставление права использования одновременно нескольким лицам (выдачу разрешения на использование – лицензии)» [5, с.114-115].

Наконец, «ослабленные абсолютные» права характеризует, помимо прочего, наличие границ по территории признания, кругу лиц, времени действия и содержанию [5, с.116]. В силу особенностей объекта данных прав, они могут быть ограничены сроком (как в силу утраты информацией актуальности, так и в силу необходимости свободного использования такой информации для развития научного и интеллектуального потенциала общества). Также, как правило, абсолютное право на информацию прекращает свое действие в случае передачи такой информации на территорию другого государства, если только такое государство не осуществляет охраны такой информации на основе принципа взаимности или в силу заключенного международного договора.

Применительно к правам на информацию необходимо выделить еще одну особенность. Характеристиками объекта права обусловлен тот факт, что право на информацию является не только «ослабленным» по сравнению с классическим абсолютным правом, но и содержащим дополнительное правомочие, а именно правомочие запрещать всем третьим лицам определенные действия в отношении объекта права. Это не означает, что право на информацию может быть сведено только к возможности запрещать, ведь целью установления исключительных прав было введение данных прав в гражданский оборот. Поэтому право на информацию – это право и разрешать (что необходимо для введения права в гражданский оборот), и запрещать (что необходимо для защиты интересов правообладателя), а также право на собственные действия по использованию информации [6, с.31].

Реализация абсолютных прав на информацию в странах ЕАЭС осуществляется в рамках режима тайны (информации ограниченного доступа), предоставления информации из информационных ресурсов и систем, а также в рамках реализации права составителя базы данных (исключительного права). Отдельный вид правового регулирования оборота информации представляет собой законодательство о персональных данных, которое, однако не может быть рассмотрено как собственно право на информацию, поскольку оно регулирует оборот данных, а не права на них. Рассмотрим указанные правовые режимы подробнее.

В рамках системы правового регулирования тайна представляет собой особый правовой институт, имеющий свою внутреннюю структуру. Структурированность данного института обусловлена двойственностью его правового понимания: это одновременно и информация определенного характера, доступ к которой ограничен, и механизм ее правовой защиты от несанкционированного доступа и распространения. При этом правовой институт тайны, как правило, носит межотраслевой характер, т.е. состоит из норм различных отраслей права.

В рамках данного института следует выделить три субинститута:

- группы норм, устанавливающих критерии и условия отнесения информации к тому или иному виду тайны (субинститут тайнообразования);
- группы норм, устанавливающих меры и механизм защиты такого рода информации (субинститут мер правовой защиты);
- группа норм, определяющих санкции за неправомерный доступ к данной информации или ее незаконное распространение (субинститут санкций).

В современном законодательстве стран ЕАЭС упоминается более 20 видов тайн [10, ст. 8; 11, ст. 17-19; 12, ст.13]. Однако далеко не для всех из них сформированы все три упомянутых выше субинститута. Более того, некоторые виды тайн существуют в законодательстве исключительно в форме упоминания о них. Так, например, в ст.23 типового Соглашения об избежании двойного налогообложения доходов и имущества (утв. Постановлением Правительства РФ от 28 мая 1992 г. N 352) говорится о невозможности ни в коем случае при обмене информацией обязать договаривающиеся государства предоставлять информацию, которая раскрывает не только коммерческую

или профессиональную тайну, но и торговую, промышленную тайну, а также торговый процесс, информацию, раскрытие которой противоречило бы государственной политике, которую нельзя получить по законодательству или в ходе обычной административной практики одного из договаривающихся государств. В заключенных на основании данного типового Соглашения двусторонних правительственных соглашениях этот перечень продублирован с добавлением новых вариаций: секретный торговый процесс, предпринимательская тайна, информация, противоречащая государственным интересам, информация, раскрытие которой противоречит национальному законодательству. Однако одного лишь упоминания недостаточно для того, чтобы можно было говорить о наличии того или иного вида тайны как правового института. Только при наличии всех трех субинститутов возможна надлежащая правовая защита информации, доступ к которой должен быть ограничен по тем или иным причинам. Причем эффективность такой защиты напрямую зависит от четкости, непротиворечивости и согласованности норм различных субинститутов между собой.

В связи с многообразием видов тайн (информации ограниченного доступа), особой структурой правового института, его межотраслевым характером, особое значение приобретает задача классификации видов информации ограниченного доступа. В отсутствие четкой классификации затрудняется отнесение информации к определенному виду тайны, что, соответственно, порождает неясность в вопросе о применяемом правовом режиме и, как следствие, о возможности оборота данного вида информации как внутри страны, так и в международном информационном обмене.

Для целей классификации видов тайн наибольшее значение имеет субинститут тайнообразования. В зависимости от особенностей данного субинститута все виды информации ограниченного доступа могут быть разделены на три группы:

1. Государственная, служебная, коммерческая тайна.

2. Профессиональные, процессуальные тайны.

3. Личная, семейная тайна, информация о частной жизни.

К первой группе следуют отнести государственную, служебную и коммерческую тайну. Особенностью субинститута тайнообразования тайн первой группы является то, что, для отнесения к ним информации недостаточно одного лишь соответствия ее какому-либо описанию. В общем случае, информация, которая может быть к ним отнесена, получает правовую охрану не с момента ее возникновения, а только после установления в отношении нее соответствующего правового режима. Порядок установления правового режима предусматривает введение в отношении информации мер по охране ее конфиденциальности, в обязательном порядке включающих нанесение на материальные носители, содержащие информацию, или проставление в сопроводительной документации на них, соответствующего грифа: «особой важности», «совершенно секретно» и «секретно» – для государственной тайны, «Коммерческая тайна» - для коммерческой тайны, или специальной пометки «Для служебного пользования» - для служебной тайны.

Иное содержание имеет субинститут тайнообразования информации второй группы. В рамках данной группы для отнесения сведений к категории информации ограниченного доступа выполнения каких-либо специальных действий не требуется, и условием, достаточным для правовой охраны информации, является ее соответствие описанию информации, относимой законом к тому или иному виду информации ограниченного доступа. В соответствии с действующим законодательством стран ЕАЭС, в рамках второй группы могут быть выделены следующие тайны. Профессиональные тайны: тайна усыновления (удочерения), врачебная (медицинская) тайна, тайна страхования, банковская тайна, налоговая тайна, тайна связи, нотариальная тайна, журналистская тайна, тайна голосования, информация о намерениях заказчика

(застройщика) по реализации архитектурного проекта, адвокатская тайна, тайна исповеди. Процессуальные тайны: тайна предварительного расследования, институт ограничения гласности судебного разбирательства (тайна закрытого судебного разбирательства), тайна совещания судей, тайна совещания и голосования присяжных заседателей. Говоря о процессуальных тайнах, хотелось бы обратить внимание, что в силу дуалистичности значения понятия «тайна» (данное понятие используется и в значении информации ограниченного доступа, и правового института, представляющего собой совокупность правовых норм, устанавливающих или допускающих ограничение доступа к информации) наименование видов тайн может не совпадать с наименованиями соответствующих видов информации ограниченного доступа. Процессуальные тайны служат тому ярким примером. Так, в рамках каждой из процессуальных тайн охраняются, соответственно следующие виды информации ограниченного доступа:

- в рамках тайны предварительного расследования – данные предварительного расследования, ставшие известные участниками уголовного судопроизводства;
- тайна закрытого судебного разбирательства – сведения, полученные участниками закрытого судебного разбирательства в ходе участия в нем;
- тайна совещания судей, – информация, представляющая собой суждения, имевшие место при обсуждении и принятия решения по делу;
- тайна совещания и голосования присяжных заседателей – информация, представляющая собой суждения, имевшие место при вынесении вердикта.

Возможна также и обратная ситуация, когда законом охраняется конфиденциальность сведений, однако к определенному виду тайны они не относятся. Таковыми являются сведения о мерах безопасности, применяемых в отношении судьи и участников уголовного процесса.

Субинститут тайнообразования для информации второй группы образуют законодательные нормы стран ЕАЭС [10, ст. 8; 11, ст. 17-19; 12, ст.13], в большинстве случаев закрепленные в виде перечня сведений, относящихся к определенному виду информации ограниченного доступа и исключений из него. В некоторых случаях, указывается только наименование тайны, это касается, например, тайны усыновления (удочерения), тайны голосования, тайны исповеди. При этом, как правило, описание сведений представляет собой указание на обстоятельства их получения определенном лицом или группой лиц, в качестве которых выступают:

- граждане (физлица), получившие информацию при исполнении ими профессиональных обязанностей, организации – при осуществлении ими определенных видов деятельности – для профессиональных тайн;
- граждане (физлица), получившие информацию в результате участия в определенных процессуальных действиях – для процессуальных тайн.

Личная и семейная тайна являются особым видом тайн. Это т.н. первичные тайны, и иные тайны как совокупность правовых норм, во многих случаях, выступают в качестве правовых гарантий конституционных прав на неприкосновенность частной жизни, личную и семейную тайну. В результате одна и та же информация о частной жизни лица, составляющая личную или семейную тайну, в зависимости от обстоятельств ее использования может охраняться в режиме иных тайн. К таким тайнам-гарантиям могут быть отнесены тайна связи, тайна усыновления (удочерения), врачебная (медицинская) тайна, тайна страхования, нотариальная тайна, адвокатская тайна, тайна исповеди, тайна закрытого судопроизводства. Следует отметить, что такое соотнесение тайн весьма условно, в связи с неопределенностью содержания понятий личная и семейная тайна. Субинститут тайнообразования для личной и семейной тайны в законодательстве стран ЕАЭС фактически состоит лишь из одного их наименования, в результате чего, во многих

случаях, вопрос о возможности отнесения тех или иных сведений к данным тайнам является довольно сложным.

Анализируя тайну как «ослабленное абсолютное» право на информацию, необходимо оговорить, что правомочия разрешать и запрещать использование такой информации носят в странах ЕАЭС неоднородный характер, различаясь в зависимость от вида тайны (группы тайн). Для тайн первой группы вопросы разрешения или запрещения ее использования урегулированы формальным образом: ограничение доступа к информации, отнесенной к гостайне, прямо установлено в законодательстве о гостайне; доступ к информации, составляющей коммерческую тайну априори ограничен, т.к. в отсутствие такого ограничения информация в принципе не может быть отнесена к коммерческой тайне; отнесение информации к служебной тайне (служебной информации ограниченного распространения), предполагает установление в отношении нее специального правового режима, включающего в себя ряд ограничений в том числе на доступ к ней: документы с пометкой "Для служебного пользования" передаются работникам подразделений под расписку, от одного работника другому – с разрешения соответствующего руководителя и т.д.

Анализ законодательства стран ЕАЭС о тайнах второй и третьей группы при этом показывает, что в нем отсутствуют нормы, регулирующие право запрещать или разрешать доступ к информации, относимой законом к профессиональным тайнам или тайне частной жизни. В большинстве случаев в отношении такой информации законом установлен только запрет на ее разглашение. Достаточно ли установления запрета на разглашение определенного рода сведений для квалификации его как наличие «ослабленного абсолютного» права на информацию? При ответе на данный вопрос необходимо учесть следующие факторы.

Во-первых, вряд ли можно признать разглашением информации действия лиц, фактически не владеющих данной информацией, по той простой причине, что, в силу отсутствия у них данной информации, они в принципе не могут ее кому-либо передать до тех пор, пока сами ее не получат. Соответственно, под разглашением тайн имеются в виду действия только того лица, которое фактически владеет информацией.

Во-вторых, отдельного внимания заслуживает закрепленная законодательством ряда стран ЕАЭС возможность ограничения распространения информации [12, ст.11; 13, ст. 6]. Например, текст документа, содержащего информацию, отнесенной к служебной тайне, должен быть доведен до сведения сотрудников определенного ведомства. Круг лиц, до сведения которых должна быть доведена информация, индивидуально не определен, но ограничен сотрудниками ведомства, т.е. фактически имеет место ограничение на распространение.

Наконец, важно закрепленное законодательством стран ЕАЭС различение распространения и предоставления информации [12, ст.14; 13, ст10]. Данные виды информационных отношений различаются между собой не только и не столько по кругу лиц, получающих информацию, сколько по тому, от кого из субъектов этих отношений исходит инициатива передачи информации. Если отвлечься от закрепленных в законодательстве стран ЕАЭС определений и обратить внимание на лексическое значение слова «предоставление», а также на те действия, которые фактически осуществляются или могут осуществляться в рамках предоставления или распространения информации, то, со всей очевидностью, обнаруживается существенное отличие в содержании этих двух понятий,. Отличие заключается в том, что предоставление информации всегда предполагает двустороннюю связь между лицом, передающим информацию и лицом, получающим ее. В данном случае передаче информации всегда предшествуют активные действия получателя, выражающиеся в запросе на получение информации либо соответствующем волеизъявлении, закрепленном в договоре между ним и лицом,

передающим информацию. При этом у стороны информационных отношений, передающей информацию, всегда существует обязанность предоставить определенного рода сведения, закрепленная в законе или являющаяся обязательством по договору. Распространение информации, напротив, всегда носит односторонний характер. В данном виде информационных отношений у получателя информации пассивная роль, для передачи информации не требуется предварительное осуществление с его стороны каких-либо действий. Более того, он может даже не желать ее получения. Также следует обратить внимание, что при некоторых способах информационного взаимодействия не происходит непосредственной передачи информации получателю. Лицо, передающее информацию, лишь создает необходимые условия для ее получения неопределенным кругом лиц или конкретным лицом, и для того, чтобы ознакомиться с данной информацией пользователь должен совершить определенные действия. Такая ситуация наиболее актуальна для распространения информации, когда некие сведения распространяются посредством СМИ, размещаются на Интернет-сайтах, на досках объявлений и т.п. Однако существует также ряд случаев, когда аналогичная модель отношений существует и в рамках предоставления информации. Так, например, лицу по его запросу может быть предоставлен доступ к закрытому фонду библиотеки, базы данных, закрытому разделу Интернет-сайта.

Обеспечение доступа к информации также необходимо рассматривать в качестве одного из вариантов предоставления или распространения информации [9, 10]. С одной стороны, обеспечение доступа к информации может быть признано ее распространением или предоставлением в связи с наличием в определениях указания на «действия, направленные на получение информации». С другой стороны, в определениях не указано, чьи именно действия должны быть направлены на получение информации. В связи с чем возникает описанная выше ситуация, когда действия лица, направленные на получение им информации, формально подпадают под определения предоставления или распространения информации, даже в том случае, когда фактической передачи сведений не состоялось.

В своей совокупности указанные обстоятельства позволяют говорить о том, что даже в отношении тайн второй и третьей группы в странах ЕАЭС действует «ослабленное абсолютное» право обладателя информации на информацию, составляющую соответствующую тайну. При этом фактически правомочия ограничены правом лица на использование информации, поскольку разрешение или запрещение использования информации другими лицами осуществляется непосредственно законом.

Но можно ли считать, что запрет на осуществление активных действий по разрешению или запрещению использования информации другими лицами является одновременно обязанностью для всех остальных лиц соблюдать режим тайны? По всей видимости, нет. Согласно общей теории права, по средствам, используемым для регулирования общественных отношений нормы права подразделяются на обязывающие, запрещающие и управомачивающие. Одна и та же норма не может быть одновременно и запрещающей и обязывающей или управомачивающей. Следовательно, законодательно закрепленный запрет на разглашение той или иной информации не возлагает на владеющее ею лицо обязанностей ограничить к ней доступ, равно как и не наделяет его правом на установление таких ограничений. При этом в законодательстве стран ЕАЭС существует понятие «конфиденциальность информации», определяемое как обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя [13, ст.2; 11, ст.1]. Именно в этом заключается суть законодательных предписаний, адресованных лицу, владеющему информацией, являющейся тайной: воздержаться от передачи этой информации кому-либо, за исключением случаев, когда владелец информации выразил согласие на ее передачу, а также случаев, прямо предусмотренных законом. В связи с

наличием именно этого требования информация может считаться той или иной тайной и соответственно подлежит правовой охране.

Исключительное право на информацию в законодательстве стран ЕАЭС основано на положениях Директивы 96/9/ЕС о правовой охране баз данных, в которой предусматривается так называемое право sui generis (право особого рода). Установленное Директивой 96/9/ЕС право особого рода предоставляет изготовителю базы данных, который внес количественно или качественно существенный вклад в получение, проверку или представление содержания базы данных, возможность запрещать изъятие или повторное использование всего содержания базы данных или его количественно/качественно существенной части. Созданная таким образом база данных получит охрану на основании права «особого рода». Иначе говоря, в рамках указанной Директивы охрана предоставляется не произведению как таковому (то есть результату творческой деятельности), а тем инвестициям, которые были вложены в создание объекта - базы данных.

Права операторов информационных систем, информационных ресурсов на последующее использование информации из таких систем и ресурсов в законодательстве стран ЕАЭС, как правило, сводятся к их исключительному праву как изготовителя базы данных. В отсутствие полноценного абсолютного права на информацию, аналогичного праву собственности, операторы информационных систем и информационных ресурсов не имеют права разрешать или запрещать использование информации, уже извлеченной из таких ресурсов и систем, что не отменяет, однако, правомочий, предоставленных им в рамках исключительного права изготовителя баз данных или в рамках режима соответствующей тайны. Тем не менее, ограничения на последующее использование информации из информационных систем и информационных ресурсов могут быть установлены напрямую законодательством стран ЕАЭС.

Таким образом, можно констатировать, что в отсутствие в законодательстве стран ЕАЭС полноценного абсолютного права на информацию, аналогичного праву собственности, права на информацию, имеющуюся в государственных информационных системах и ресурсах, доступа к государственным информационным системам органов власти государств-членов и систем, связанных с оборотом данных в рамках ЕАЭС, и иных заинтересованных субъектов можно охарактеризовать как ослабленные абсолютные права, существующие либо в виде исключительного права изготовителя базы данных в случаях, когда такое право признается законодательством соответствующей страны ЕАЭС, либо в виде права доступа или запрета на разглашение информации в рамках соответствующей тайны. За рамками собственно прав на информацию остаются ограничения, связанные с последующим использованием информации, а также правила правового режима информации, не связанные с наличием абсолютного или ослабленного абсолютного права, накладывающие ограничения на последующее использование и передачу информации из информационных ресурсов и систем, в том числе государственных.

СПИСОК ИСТОЧНИКОВ:

1. Радько Т.Н., Лазарев В.В., Морозова Л.А. Теория государства и права. Учебник для бакалавров. М., 2016

2. Грибанов В.П. Осуществление и защита гражданских прав. М., 2003.

3. Братусь С.Н. Субъекты гражданского права. Л., 1950.

4. Иоффе О.С. Избранные труды по гражданскому праву. М., 2003.

5. Дозорцев В.А. Интеллектуальные права: понятие. Система. Задачи кодификации. Сб.статей. М., 2005.

6. Зенин И.А. Исключительное интеллектуальное право (право интеллектуальной собственности) как предмет гражданского оборота // Законодательство. 2008. № 8.

7. Закон Республики Казахстан от 15 марта 1999 г. «О государственных секретах».

8. Закон Кыргызской Республики от 30 марта 1998 года «О коммерческой тайне»

9. Закон Республики Казахстан от 16 ноября 2015 г. «О доступе к информации»

10. Закон Республики Армения от 23 сентября 2003 года «О свободе информации»

11. Закон Республики Беларусь от 10 ноября 2008 года «Об информации, информатизации и защите информации»

12. Закон Кыргызской Республики от 19 июля 2017 года «Об электронном управлении»

13. Федеральный закон РФ от 27 июля 2006 г. "Об информации, информационных технологиях и о защите информации"

4. ПРАВОВОЕ РЕГУЛИРОВАНИЕ ДАННЫХ, СВЯЗАННЫХ С ЛИЧНОСТЬЮ ФИЗИЧЕСКОГО ЛИЦА, В СТРАНАХ БЫВШЕГО СССР

Наличие законодательства о защите персональных данных является требованием, соблюдение которого неизбежно для стран, взаимодействующих с Евросоюзом. На текущий момент такое законодательство тем более развито, чем ближе страна к Европе – временным исключением из этого правила является только Республика Беларусь. Но хотя дистанция, пройденная в этом направлении, разная для разных государств, проблемы, с которыми они сталкиваются, схожи. Рассмотрим их подробнее.

Действующее законодательство стран бывшего СССР по вопросам защиты персональных данных представлено следующими актами:

Республика Армения - Закон от 13 июня 2015 года №ЗР-49 «О защите персональных данных»

Республика Беларусь – профильный закон отсутствует, основу законодательства о персональных данных составляют Закон Республики Беларусь 21.06.2008 № 418-З «О регистре населения», Закон Республики Беларусь от 10 ноября 2008 г. № 455-З «Об информации, информатизации и защите информации», Закон Республики Беларусь от 13 июля 2006 г. № 144-З «О переписи населения». Разработка закона о персональных данных предусмотрена утвержденным планом законотворчества на 2018 год.

Республика Молдова – закон от 8 июля 2011 года №133 «О защите персональных данных»

Республика Казахстан - закон от 21 мая 2013 года № 94-V «О персональных данных и их защите»

Кыргызская Республика – закон от 14 апреля 2008 года № 58 «Об информации персонального характера»

Российская Федерация – Федеральный закон от 27 июля 2006 года № 152-ФЗ «О персональных данных»

Республика Таджикистан – профильный закон отсутствует, отдельные положения о защите персональных данных содержат Закон Республики Таджикистан от 10 мая 2002 года №55 «Об информации» и Закон Республики Таджикистан от 2 декабря 2002 года №71 «О защите информации»

Уполномоченный орган. При назначении государственного органа, уполномоченного на защиту прав субъектов персональных данных, все страны отталкиваются от положений Дополнительного протокола к Конвенции о защите физических лиц при автоматизированной обработке персональных данных, о наблюдательных органах и трансграничной передаче информации (Страсбург, 8 ноября 2001 г.). В соответствии с ним, такой орган должен иметь полномочия проводить расследования, вмешиваться, а также принимать участие в юридических процессах или акцентировать внимание компетентных судебных органов на нарушении национального права. Кроме того, такой орган должен осуществлять свои функции абсолютно независимо, что подразумевает достаточно высокий статус в системе государственных органов.

Для постсоветской государственности, однако, статус любого государственного органа неразрывно связан с его влиянием на политику государства в целом. В разных государствах это могут быть министерства экономики, финансов, силовые ведомства – то есть органы, имеющие реальные возможности по осуществлению государственной власти. Но орган, защищающий персональные данные, – зачем давать ему высокий статус, если осуществляемая им функция является для государства второстепенной? По этой причине, например, Роскомнадзор – уполномоченный орган в России – так и не выведен даже на уровень Правительства и находится в подчинении Министра цифрового развития, связи и массовых коммуникаций. Руководство Роскомнадзора – хотя ведомство занимается не только персональными данными, а еще и контролем за Интернетом – так и не смогло набрать политический вес, равный силовым министерствам и правоохранительным органам. Аналогичный Роскомнадзору статус имеет и уполномоченный орган Армении – Агентство по защите персональных данных Министерства юстиции.

В Центральной Азии понимание защиты персональных данных как существенной, но все же не жизненно важной функции государства приводит к другой проблеме с созданием уполномоченного органа: на него просто нет денег в государственном бюджете. Из-за этого до сих пор не назначен уполномоченный орган в Кыргызстане; задержка с принятием законодательства о персональных данных в Таджикистане также связана с нежеланием выделять деньги на реализацию новых полномочий или созданием новых органов. Сложно судить, насколько повлиял на решение данного вопроса в Казахстане финансовый фактор, но и там орган, уполномоченный сфере защиты персональных данных, законодательством не определен.

Уведомление. Обязанность операторов персональных данных направлять уведомление о начале обработки не предусмотрена ни Конвенцией, ни Дополнительным протоколом к ней. В силу этого институт уведомления не является императивным даже для государств, ратифицировавших Конвенцию. Однако во многих странах постсоветского пространства, принявших у себя законы о защите персональных данных, обязанность направлять уведомление присутствует – например, в России, Армении и Кыргызстане (впрочем, в Кыргызстане фактически уведомлять некого – в отсутствие уполномоченного органа).

Факт направления уведомления ставит оператора персональных данных под административный надзор уполномоченного органа. Кроме того, как минимум, в России уведомление предполагает раскрытие значительного перечня информации (в том числе о мерах по защите персональных данных), которая должна обновляться по мере ее изменения. Эти два фактора ведут к тому, что операторы всячески оттягивают момент направления уведомления или пытаются не направлять его вообще, используя исключения, установленные в законе.

В результате уведомление превращается в своего рода бюрократический фетиш: ведение реестра операторов персональных данных является функцией уполномоченного органа, на которую он затрачивает трудовые ресурсы. При этом сами операторы не заинтересованы в направлении уведомления – как следствие, дополнительные ресурсы уполномоченного органа тратятся на принуждение (убеждение) операторов. С учетом ограниченности ресурсов, выделяемых на деятельность уполномоченного органа, это отвлекает его от основной задачи – защиты прав субъектов персональных данных, зато позволяет демонстрировать успехи в отчетности: сколько операторов выявлено, поставлено на учет, привлечено к ответственности за ненаправление уведомления и т.п.

Централизация государственных данных. Для персональных данных можно использовать аналогию с радиоактивными веществами. При небольшой их концентрации риска взрыва нет. Но при достижении некоей критической массы начинается цепная реакция, которая, в отсутствие управления ею, неизбежно приводит к взрыву. Ценность персональных данных, особенно с учетом технологий Big Data, возрастает экспоненциально в зависимости от объема совместно хранимых данных. Так же по экспоненте растут и расходы на меры по обеспечению безопасности обрабатываемых данных.

Реализация законодательства о защите персональных данных на постсоветском пространстве совпадает – по времени и по сути – с созданием электронного правительства. При создании электронного правительства неизбежно возникает вопрос о централизации хранимых данных, который в разных странах решается по-разному именно из-за проблем безопасности хранимых данных. С одной стороны, централизация данных (создание единого реестра населения, единой информационной системы, в которой осуществляется обработка персональных данных в рамках электронного правительства), позволяет уменьшить затраты, устранить проблему несоответствий между данными разных ведомств, централизованно управлять безопасностью данных. С другой стороны, нарушение безопасности такой информационной системы опаснее нарушения безопасности одной из многих систем государственных органов, обрабатывающих данные для выполнения собственных функций.

Хотя в российском законодательстве еще в 2006 году предусматривалось создание государственного регистра населения, до настоящего момента такой регистр не создан именно из-за опасений, связанных с информационной безопасностью. Предпринимаются меры лишь по переводу в электронный вид государственных услуг, оказываемых органами записи актов гражданского состояния – и то по состоянию на начало 2018 года этот процесс не завершен.

Радикально иной путь был выбран в Молдове, где все данные о гражданах были объединены в рамках Центра государственных информационных ресурсов "Registru". Наличие единых государственных регистров населения, правовых единиц, водителей и транспорта позволило сравнительно быстро создать систему электронного правительства, однако ставит вопрос о защищенности таких данных. Ведь аналогичная система, созданная в Кыргызстане в рамках закона о биометрической регистрации, как выяснилось, не позволила обеспечить надлежащий уровень безопасности данных. Данные, собранные в ходе биометрической регистрации, в частности, оказывались опубликованными на сайтах в интернете.

Технические меры защиты. Статья 7 Конвенции говорит о том, что для защиты персональных данных должны приниматься надлежащие меры безопасности, направленные на предотвращение их случайного или несанкционированного уничтожения или случайной потери, а также на предотвращение несанкционированного доступа, их изменения или распространения таких данных. При имплементации этого требования в

национальных законодательствах стран Евразии законодатель оказался перед выбором: конкретизировать или нет требования по защите информации.

Российское законодательство, где сильны традиции правового регулирования мер технической защиты информации, вначале пошло по пути жестких требований к безопасности персональных данных, обязательных для всех операторов – такие требования были введены с 2008 года. Однако уже в 2011 сфера обязательных требований была фактически сужена до государственных информационных систем. Формально, конечно, требования распространяются на всех, но контролируются только для государственных операторов.

Схожий подход, предполагающий нормативную детализацию мер по технической защите, предусмотрен в Армении, однако подзаконные акты, которыми предполагается установить требования по информационной безопасности, так и не приняты. В законодательстве Кыргызстана требования по информационной безопасности носят достаточно лаконичный характер, устанавливая уровни защищенности (каждый из которых обозначается своим цветом) и соответствующие им требования по защите данных. Законодательство Казахстана, напротив, устанавливает лишь цели защиты и собственно обязанность оператора обеспечивать такую защиты, оставляя конкретные меры защиты на усмотрение оператора.

Реализация подхода, основанного на нормативном установлении требований к защите персональных данных, затруднена в силу отраслевой специфики: в каждой отрасли данные и угрозы для них разные. В силу этого все большее понимание на постсоветском пространстве находят идеи privacy by design, то есть защиты данных на уровне архитектур информационных систем, а не как внешнего по отношению к системе требования или приложения. Однако переход к этим принципам – и то лишь в отношении государственных информационных систем – только намечается. Например, этот подход можно заметить в новом законе Казахстана об информатизации, вступившем в силу в 2016 году.

Ответственность. Особенностью законодательства о персональных данных стран постсоветского пространства является отнесение правонарушений, связанных с обработкой персональных данных, к числу публично-правовых (административных или уголовных). Ответственность (как правило, в виде штрафа) наступает за нарушение правил обработки персональных данных, штраф взыскивается в пользу государства. Ответственность в пользу потерпевших (возмещение убытков или морального вреда) зачастую предусмотрена (например, в России и Кыргызстане), но механизм привлечения к такой ответственности не детализирован, в силу чего пострадавшим гражданам приходится обращаться в суд за возмещением морального вреда самостоятельно и самостоятельно же собирать доказательства.

В рассмотренных странах можно наблюдать четкое понимание законодательства о персональных данных как составной части административного права, со всеми вытекающими отсюда особенностями и проблемами. Уполномоченные органы в большей степени сосредоточены на осуществлении бюрократических процедур, а не на реальной защите интересов граждан, операторы персональных данных (как частные, так и государственные), больше боятся проверок, чем утечек данных. Попытки административным путем заставить операторов защищать данные неудачны, как в силу специфики самих процессов обработки данных, их «встроенности» в другие бизнес-процессы, так и в силу отсутствия мотивации у операторов защищать данные. В целом государствами Евразии персональные данные граждан рассматриваются больше как государственная собственность, нежели как информация, права на которую имеют сами граждане.

Нельзя сказать, что виноваты в таком подходе национальные законодатели. Скорее нет. Нельзя также сказать, что отсутствие эффективной защиты персональных данных является следствием какого-то нигилизма, беззаботного отношения к персональным данным, допустим, являющегося наследием советской эпохи. По-видимому, текущие проблемы с защитой персональных данных вызваны сменой парадигмы защиты. От существовавшей в советское время гражданско-правовой защиты частной жизни лица, эквивалентной, скорее, институту privacy в США, страны бывшего СССР переходят к европейской парадигме защиты персональных данных как таковых, причем переходят вынужденно, из-за давления ЕС. При этом такой переход осуществляется «сверху», по административным каналам и в угоду административным же целям сотрудничества между странами ЕС и постсоветскими странами.

Как результат, законодательство о персональных данных ЕС переписывается под копирку, без осознания того, что в ЕС персональные данные – это товар для огромного рынка, с рыночными законами и рыночной ответственностью, где государство лишь устраняет так называемые market failures, но не мешает рыночному саморегулированию. Законодательство о персональных данных постсоветских стран, напротив, максимально выводит персональные данные из рыночного оборота, ограничивая их передачу и использование. Одни и те же механизмы, понимаемые по-разному, приводят к принципиально различным последствиям.

Так что политика в сфере защиты персональных данных на постсоветском пространстве находится только в начале большого пути. Да, законодательство написано, но оно еще не стало правилами игры, понятными гражданам и бизнесу, не привело к такому состоянию общественных отношений, где граждане заинтересованы делиться данными, необходимыми для бизнеса и электронного правительства, а операторы заинтересованы в максимальной защите таких данных и – это важнее всего – не заинтересованы во вторжении в личную, интимную сферу граждан.

5. ПРЕДЛОЖЕНИЯ ПО ИЗМЕНЕНИЮ ЗАКОНОДАТЕЛЬСТВА В ЦЕЛЯХ СОЗДАНИЯ УСЛОВИЙ ДЛЯ УПРАВЛЕНИЯ ПРАВАМИ НА РЕЗУЛЬТАТЫ ИНТЕЛЛЕКТУАЛЬНОЙ ДЕЯТЕЛЬНОСТИ, НЕПОСРЕДСТВЕННО СВЯЗАННЫЕ С ЛИЧНОСТЬЮ ФИЗИЧЕСКОГО ЛИЦА

В связи с важностью вопросов идентификации физических лиц для решения проблемы управления правами на результаты интеллектуальной деятельности, непосредственно связанные с личностью физического лица, и отсутствием регулирования данных вопросов в действующем законодательстве, по результатам НИР были разработаны предложения в законодательство, приведенные ниже.

Статья. Идентификаторы

1. Идентификатором признается любая уникальная информация (код, шифр), однозначно связывающая лицо, вещь или процесс (далее – объект идентификации) с записью о нем в документе или информационной системе. Идентификаторы могут быть использованы для идентификации в юридически значимых целях.

2. Если не доказано иное, все записи, содержащие один и тот же идентификатор, относятся к одному и тому же объекту идентификации. Записи, содержащие разные идентификаторы, относятся к разным объектам идентификации, пока не доказано иное.

3. Положения настоящего закона об обработке персональных данных применяются к идентификаторам физических лиц в части, не противоречащей положениям настоящей статьи и положениям, относящимся к электронному удостоверению личности.

4. Публичными идентификаторами являются идентификаторы, используемые в государственных и совместных информационных системах, а также идентификаторы, используемые для обмена информацией между информационными системами общего пользования. Иные идентификаторы признаются частными идентификаторами.

5. К публичным идентификаторам физического лица относятся, в частности:

а) фамилия, имя, отчество, дата рождения;

б) идентификационный номер налогоплательщика;

в) страховой номер индивидуального лицевого счёта застрахованного лица в системе обязательного пенсионного страхования (СНИЛС);

г) квалифицированная электронная подпись;

д) абонентский номер физического лица, заключившего в установленном настоящим Кодексом порядке договор на оказание ему услуг связи.

6. К публичным идентификаторам юридического лица относятся, в частности:

а) идентификационный номер налогоплательщика;

б) основной государственный регистрационный номер или код иностранной организации;

в) квалифицированная электронная подпись.

7. В случае, когда законом, иным правовым актом или обычаем делового оборота предусмотрено требование о самоидентификации лица, то есть о раскрытии им идентификатора, однозначно указывающего на его личность, такое требование считается исполненным с момента предоставления лицом, к которому относится требование о самоидентификации, соответствующего идентификатора иным участникам информационного взаимодействия.

Статья. Электронное удостоверение личности

1. В случаях, когда законом, принятым в соответствии с ним иным нормативным правовым актом или договором установлено требование об удостоверении личности, такое удостоверение может быть совершено в электронном виде (электронное удостоверение личности) в порядке, установленном настоящей статьей. Если иное не установлено законом, иным нормативным правовым актом или договором, электронное удостоверение личности при обращении за получением электронных государственных услуг или при совершении сделки признается надлежащим волеизъявлением лица на получение электронной государственной услуги или совершение сделки.

2. Электронное удостоверение личности осуществляется в рамках системы идентификации. Система идентификации создается на основании решения оператора системы идентификации, соглашения участников системы идентификации либо нормативного правового акта. В таком решении (соглашении, нормативном правовом акте) должны быть закреплены:

а) перечень видов отношений, в которых осуществляется электронное удостоверение личности в соответствии с данной системой идентификации;

б) перечень используемых в системе идентификации идентификаторов;

в) факторы, используемые для удостоверения личности применительно к каждому из идентификаторов (в частности, ввод секретного или одноразового пароля, в том числе полученного в коротком текстовом сообщении либо иным способом с использованием

абонентского номера физического лица; использование электронной подписи; использование биометрических данных; предъявление материального носителя с определенной информацией);

г) порядок создания и(или) распределения средств идентификации (таких, как секретный или одноразовый пароль, материальный носитель с определенной информацией, ключ электронной подписи и другие);

д) процедура проверки факторов, используемых для удостоверения личности;

е) основания для принятия решения об удостоверении личности, то есть об установлении однозначной связи объекта идентификации – физического лица с идентификатором;

ж) порядок фиксации фактов электронного удостоверения личности и порядок обеспечения целостности информации о фактах электронного удостоверения личности.

3. Электронное удостоверение личности может осуществляться для собственных нужд оператора системы идентификации либо проводиться оператором системы идентификации по заказу иных лиц на основании закона, иного нормативного правового акта или соглашения между оператором системы идентификации и такими лицами. В таком законе, ином нормативном правовом акте, или соглашении участников информационного взаимодействия должны быть предусмотрены:

- порядок получения информации о факторах, используемых для удостоверения личности, и об идентификаторах;

- перечень информации, предоставляемой заказчику идентификации оператором системы идентификации по результатам электронного удостоверения личности, и условия использования такой информации;

- требования к защите информации в ходе обмена ею в процессе электронного удостоверения личности;

- условие о размере или порядке определения вознаграждения оператору системы идентификации, либо условие о безвозмездности электронного удостоверения личности.

4. Системы идентификации, использующие публичные идентификаторы, должны ежегодно проходить независимый аудит в порядке, установленном документом о создании системы идентификации.

5. Электронное удостоверение личности может быть произведено с использованием сведений, содержащихся в базах данных операторов связи, с использованием Единой системы идентификации и аутентификации, а также с использованием иных систем идентификации.

Статья. Удостоверение личности граждан Российской Федерации с использованием единой системы идентификации и аутентификации и биометрической системы

1. Государственные органы, банки и иные организации в случаях, определенных федеральными законами, после удостоверения личности при личном присутствии гражданина Российской Федерации с его согласия на безвозмездной основе размещают в электронной форме:

1) сведения, необходимые для регистрации гражданина Российской Федерации в единой системе идентификации и аутентификации, и иные сведения, если такие сведения предусмотрены федеральными законами, - в единой системе идентификации и аутентификации;

2) биометрические персональные данные гражданина Российской Федерации - в информационных системах персональных данных, обеспечивающих обработку, включая сбор и хранение биометрических персональных данных, их проверку и передачу информации о степени их соответствия предоставленным биометрическим персональным данным гражданина Российской Федерации (далее - биометрические системы).

2. Правительство Российской Федерации по согласованию с Центральным банком Российской Федерации устанавливает требования:

1) к фиксированию действий при размещении сведений, указанных в пунктах 1 и 2 части 1 настоящей статьи;

2) к проведению государственными органами и организациями, указанными в части 1 настоящей статьи, удостоверения личности гражданина Российской Федерации, за исключением организаций, проводящих идентификацию в порядке, установленном Федеральным законом от 7 августа 2001 года N 115-ФЗ "О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма".

3. Федеральные законы, устанавливающие обязанность государственных органов и организаций по размещению сведений, указанных в пунктах 1 и 2 части 1 настоящей статьи, должны предусматривать осуществление контроля и надзора за соответствующими действиями, а также определение органа государственной власти или организации, уполномоченных на их осуществление.

4. Сведения, указанные в пунктах 1 и 2 части 1 настоящей статьи, размещаются соответственно в единой системе идентификации и аутентификации и в биометрических системах уполномоченным сотрудником государственного органа или организации и подписываются усиленной квалифицированной электронной подписью такого государственного органа или организации.

5. Форма согласия на обработку персональных данных и биометрических персональных данных, указанных в пунктах 1 и 2 части 1 настоящей статьи, утверждается Правительством Российской Федерации.

6. Порядок регистрации гражданина Российской Федерации в единой системе идентификации и аутентификации, включая состав сведений, необходимых для регистрации гражданина Российской Федерации в указанной системе, порядок и сроки проверки и обновления сведений, размещаемых в единой системе идентификации и аутентификации с использованием государственных информационных систем, устанавливаются Правительством Российской Федерации. Федеральные органы исполнительной власти, в том числе федеральный орган исполнительной власти, осуществляющий функции по выработке и реализации государственной политики и нормативно-правовому регулированию в сфере внутренних дел, органы государственных внебюджетных фондов направляют в единую систему идентификации и аутентификации сведения о гражданах Российской Федерации в целях их обновления в соответствии с указанным порядком.

7. В случаях, установленных федеральными законами, государственные органы и организации вправе обновлять информацию о гражданах Российской Федерации, идентифицированных в соответствии с частью 18 настоящей статьи, с использованием сведений, полученных из единой системы идентификации и аутентификации.

8. Состав сведений, размещаемых в биометрических системах, включая вид биометрических персональных данных, определяется Правительством Российской Федерации.

9. Обработка биометрических персональных данных в государственных органах, банках и иных организациях, указанных в абзаце первом части 1 настоящей статьи, в том

числе с использованием биометрических систем, осуществляется в соответствии с требованиями к защите биометрических персональных данных, установленными в соответствии со статьей XX настоящего Кодекса.

10. Контроль и надзор за выполнением организационных и технических мер по обеспечению безопасности персональных данных, установленных в соответствии со статьей XX настоящего Кодекса, при обработке персональных данных в биометрических системах, за исключением контроля и надзора за выполнением банками организационных и технических мер по обеспечению безопасности персональных данных при использовании биометрических систем, осуществляются федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации, в пределах их полномочий, установленных законодательством Российской Федерации о персональных данных.

11. Контроль и надзор за выполнением банками организационных и технических мер по обеспечению безопасности персональных данных при использовании биометрических систем осуществляются Центральным банком Российской Федерации.

12. Правительство Российской Федерации определяет федеральный орган исполнительной власти, осуществляющий регулирование в сфере идентификации граждан Российской Федерации на основе биометрических персональных данных.

13. Федеральный орган исполнительной власти, осуществляющий регулирование в сфере идентификации граждан Российской Федерации на основе биометрических персональных данных:

1) определяет порядок обработки, включая сбор и хранение, параметров биометрических персональных данных в целях идентификации, порядок размещения и обновления биометрических персональных данных в биометрических системах, а также требования к информационным технологиям и техническим средствам, предназначенным для обработки биометрических персональных данных в целях проведения идентификации (в банковской сфере и иных сферах финансового рынка указанные требования устанавливаются по согласованию с Центральным банком Российской Федерации);

2) определяет формы подтверждения соответствия информационных технологий и технических средств, предназначенных для обработки биометрических персональных данных в целях проведения идентификации, требованиям, определенным в соответствии с пунктом 1 настоящей части, и публикует перечень технологий и средств, имеющих подтверждение соответствия (в банковской сфере и иных сферах финансового рынка формы подтверждения соответствия устанавливаются по согласованию с Центральным банком Российской Федерации);

3) разрабатывает и утверждает методики проверки соответствия предоставленных биометрических персональных данных физического лица его биометрическим персональным данным, содержащимся в биометрических системах, а также определяет степень взаимного соответствия указанных биометрических персональных данных, достаточную для проведения идентификации, предусмотренной настоящим Федеральным законом.

14. Центральный банк Российской Федерации совместно с операторами е биометрических систем определяет перечень угроз безопасности, актуальных при обработке, включая сбор и хранение, биометрических персональных данных, их проверке и передаче информации о степени их соответствия предоставленным биометрическим персональным данным гражданина Российской Федерации в государственных органах, банках и иных организациях, указанных в абзаце первом части 1 настоящей статьи, в

биометрических системах с учетом оценки возможного вреда, проведенной в соответствии с законодательством Российской Федерации о персональных данных, и согласовывает указанный перечень с федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации.

15. Государственные органы, банки и иные организации, указанные в абзаце первом части 1 настоящей статьи, операторы биометрических систем при обработке, включая сбор и хранение, биометрических персональных данных, их проверке и определении степени их соответствия предоставленным биометрическим персональным данным гражданина Российской Федерации:

1) осуществляют свои функции в соответствии с законодательством Российской Федерации о персональных данных и требованиями настоящего Федерального закона;

2) осуществляют обработку, включая сбор и хранение, биометрических персональных данных с применением информационных технологий и технических средств, имеющих подтверждение соответствия требованиям, установленным в соответствии с настоящим Федеральным законом;

3) обеспечивают проверку соответствия предоставленных биометрических персональных данных гражданина Российской Федерации его биометрическим персональным данным согласно методикам, утвержденным в соответствии с настоящим Федеральным законом.

16. Оператор биометрической системы:

1) осуществляет передачу информации о результатах проверки соответствия предоставленных биометрических персональных данных гражданина Российской Федерации его биометрическим персональным данным, содержащимся в биометрической системе, в государственные органы, банки и иные организации, указанные в абзаце первом части 1 настоящей статьи;

2) предоставляет в федеральный орган исполнительной власти, осуществляющий функции по выработке и реализации государственной политики и нормативно-правовому регулированию в сфере внутренних дел, и федеральный орган исполнительной власти в области обеспечения безопасности в целях обеспечения обороны страны, безопасности государства, охраны правопорядка и противодействия терроризму сведения, содержащиеся в биометрической системе, в порядке, установленном Правительством Российской Федерации.

17. Требования к операторам биометрической системы устанавливаются Правительством Российской Федерации.

18. Удостоверение личности гражданина Российской Федерации с применением единой системы идентификации и аутентификации, биометрических систем осуществляется без его личного присутствия в случаях, установленных федеральными законами, путем предоставления государственным органам и организациям:

1) сведений о гражданине Российской Федерации, размещенных в единой системе идентификации и аутентификации, в порядке, установленном Правительством Российской Федерации;

2) информации о степени соответствия предоставленных биометрических персональных данных гражданина Российской Федерации его биометрическим персональным данным, содержащимся в биометрической системе.

19. При предоставлении биометрических персональных данных физического лица по каналам связи в целях удостоверения его личности без личного присутствия посредством сети "Интернет" должны применяться шифровальные (криптографические) средства, позволяющие обеспечить безопасность передаваемых данных от угроз безопасности, актуальных при обработке биометрических персональных данных, определенных в соответствии с частью 14 настоящей статьи, и имеющие подтверждение соответствия требованиям, установленным в соответствии со статьей XX настоящего закона. Государственный орган, банк или иная организация, указанные в абзаце первом части 1 настоящей статьи, обязаны предложить использовать указанные средства физическим лицам, обратившимся к ним в целях проведения идентификации без личного присутствия, и указать страницу сайта в сети "Интернет", с которой предоставляются эти средства.

20. В случае, если физическое лицо для предоставления своих биометрических персональных данных в целях удостоверения его личности без личного присутствия посредством сети «Интернет» использует мобильный телефон, смартфон или планшетный компьютер и отказывается от использования шифровальных (криптографических) средств, указанных в части 19 настоящей статьи, государственный орган, банк или иная организация, указанные в абзаце первом части 1 настоящей статьи, обязаны отказать такому лицу в проведении указанной идентификации.

21. В случае, если физическое лицо при предоставлении своих биометрических персональных данных в целях удостоверения его личности без личного присутствия посредством сети "Интернет" использует иные устройства, в том числе персональный компьютер, и отказывается от применения шифровальных (криптографических) средств, указанных в части 19 настоящей статьи, государственный орган, банк или иная организация, указанные в абзаце первом части 1 настоящей статьи, уведомляет его о рисках, связанных с таким отказом. После подтверждения физическим лицом своего решения государственный орган, банк или иная организация, указанные в абзаце первом части 1 настоящей статьи, может провести соответствующую идентификацию физического лица посредством сети "Интернет" без использования им указанных шифровальных (криптографических) средств.

22. Государственные органы, банки и иные организации при удостоверении личности гражданина Российской Федерации с применением информационных технологий в соответствии с частью 18 настоящей статьи вправе подтверждать достоверность сведений, предусмотренных пунктом 1 части 18 настоящей статьи, с использованием информационных систем государственных органов, в том числе федерального органа исполнительной власти, осуществляющего функции по выработке и реализации государственной политики и нормативно-правовому регулированию в сфере внутренних дел, Пенсионного фонда Российской Федерации, Федерального фонда обязательного медицинского страхования и (или) государственной информационной системы, определенной Правительством Российской Федерации.

23. Согласие гражданина Российской Федерации на обработку персональных данных, содержащихся в единой системе идентификации и аутентификации, и биометрических персональных данных для проведения его идентификации с применением информационных технологий в соответствии с частью 18 настоящей статьи может быть подписано его простой электронной подписью, ключ которой получен в соответствии с правилами использования простой электронной подписи при обращении за получением государственных и муниципальных услуг в электронной форме, установленными Правительством Российской Федерации. Указанное согласие, подписанное простой электронной подписью, признается электронным документом, равнозначным документу на бумажном носителе, подписанному собственноручной подписью данного гражданина Российской Федерации.

24. Размер и порядок взимания оператором биометрической системы платы за предоставление государственным органам и организациям сведений, указанных в пункте 2 части 18 настоящей статьи, определяются федеральным органом исполнительной власти, осуществляющим функции по выработке и реализации государственной политики и нормативно-правовому регулированию в сфере информационных технологий, по согласованию с оператором биометрической системы и иными государственными органами и организациями в случаях, установленных федеральными законами.